jamk.fi

Examination of contemporary cyber security education

Jaakko Backlund

Master's thesis
May 2020
School of Technology, Communication and Transport
Master's Degree Programme in Information Technology
Cyber Security

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

jamk.fi

Kuvailulehti

Tekijä(t)	Julkaisun laji	Päivämäärä
Backlund, Jaakko	Opinnäytetyö, ylempi AMK	06 2020
	Sivumäärä 128	Julkaisun kieli Englanti
		Verkkojulkaisulupa myönnetty: x

Työn nimi

Nykyaikaisen kyberturvallisuuskoulutuksen katsaus

Tutkinto-ohjelma

Information Technology

Työn ohjaaja(t)

Jarmo Nevala; Tero Kokkonen

Toimeksiantaja(t)

Karo Saharinen, JAMK, Cyber Security for Europe -projekti

Tiivistelmä

Jyväskylän ammattikorkeakoulu toimii osana Cyber Security for Europe -projektia, jonka tarkoituksena on kehittää sekä yhtenäistää Euroopan maiden kyberturvallisuuskykyjä, kehittää kyberturvallisuuden hallintaa sekä vähentää kyberturvallisuusosaamisen sekä kyberturvallisuusosaamisen tarpeen välistä kuilua. Kyberturvallisuusosaamisen jatkuvasti kasvava tarve sekä tarpeen ja ammattitaitoisten asiantuntijoiden kasvava ero on herättänyt tarpeen tarkastella koulutusohjelmien tarjontaa sekä mahdollisuuksia kehittää koulutusohjelmia vastaamaan paremmin työelämän vaatimuksia.

Tutkimuksen tarkoituksena oli selvittää, vastaavatko kyberturvallisuusalan koulutusohjelmat työelämän sidosryhmien tarpeita sekä tarkastella, joutuuko opintotarjonnassa heikompaan asemaan jokin kyberturvallisuuden alue, jonka sidosryhmät kokevat tärkeäksi osa-alueeksi. Tutkimus suoritettiin keräämällä kyberturvallisuuskoulutusohjelmien kurssitiedot painottuen saatavuuteen sekä haastattelemalla kyberturvallisuuden parissa työskenteleviä ammattilaisia. Haastattelutuloksia vertailtiin kerättyyn kurssidataan ja näiden tulosten perusteella tehtiin johtopäätökset, vastaako koulutusohjelmien tarjonta sidosryhmien tarpeita.

Kyberturvallisuuskoulutuksen saatavuus eri osa-alueilla oli vaihtelevaa, mutta pääsääntöisesti saatavuus vastasi kysyntää tärkeimmillä osa-alueilla. Sidosryhmien tarpeet ja vertailu kurssidataan paljasti useita eri lähestymiskohtia koulutuksen kehittämiselle. Yhdeksi vahvimmista kehityskohteista muodostui verkko- ja ohjelmointiosaamisen parantaminen kyberturvallisuuskoulutuksessa, mahdollisesti erimerkiksi kerrostamalla koulutusohjelmat verkko- tai ohjelmointikoulutuksen päälle. Tutkimuksen aikana ilmeni useita tarpeita jatkotutkimuksille, jotta tutkimuskysymyksiin voitaisiin vastata vedenpitävästi.

Avainsanat (asiasanat)

Opinto-ohjelmavertailu, kyberturvallisuuden tarpeet, koulutus, NCWF

Muut tiedot (salassa pidettävät liitteet)

jamk.fi

Description

Author(s)	Type of publication	Date
Backlund, Jaakko	Master's thesis	06 2020
		Language of publication: English
	Number of pages: 128	Permission for web publication: x

Title of publication
Examination of contemporary cyber security education

Degree programme
Master's degree programme in Information Technology

Supervisor(s)
Nevala Jarmo; Kokkonen Tero

Assigned by
Karo Saharinen, JAMK, Cyber Security For Europe -project

Abstract

Jyväskylä University of Applied Science is part of the Cyber Security for Europe project, which aims to develop and unify the cyber security capabilities of European countries, develop cyber security management, and reduce the gap between cyber security expertise and demand. The ever-growing demand for cyber security expertise and the growing gap between the availability and demand for skilled experts have raised the need to examine the offering of education programmes as well as the opportunities to develop education programmes to better meet the demands of working life.

The purpose of the study is to find out whether cyber security degree programmes meet the demands of stakeholders and to examine whether an area of cybersecurity perceived by stakeholders as an important area is at a disadvantage in degree curriculums. The study was conducted by collecting course data from cyber security degree programmes with an emphasis on the availability of courses and by interviewing professionals working in cyber security, on the basis of which a comparison was made with the collected course data.

The availability of cybersecurity education in different areas showed variation, but as a rule, the availability corresponded to the demand in the most important areas. Stakeholder needs as well as comparison of course data revealed several different approaches to the development of cybersecurity education. One of the strongest areas of development was the improvement of network and programming skills in cybersecurity education, possibly by layering degree programmes on top of network or programming degree programmes. During the study, several needs for further research emerged to provide a clearer answer to the research questions.

Keywords/tags (subjects)
Curriculum comparison, stakeholder demands on cyber security, education, NCWF

Miscellaneous

Contents

Figures

Tables

1 Introduction

The evolution of Information Technology and the Internet has transformed human lives and habits during the 21st century. Many services which earlier required visiting physical locations or establishments are now available from anywhere and at any time (Digital Services N.d).

Social interactions increasingly move to social media platforms, and according to the Bank of Finland (2019), money transactions are completed on electronical platforms in an ever-increasing volume.

Information technology was utilized before the 21st century as well, but during that time, the assets containing information and data had next to no connectivity to public networks outside of the company's internal network. Presently, this situation has changed. People demand services outside of office hours, and companies and bureaus answer to this demand by providing their services over different mediums, internet being one of the most common mediums (Digitalisation N.d; Salminen, M. 2014).

As Information Technology and the Internet landscape has developed, technology has provided people with the ability to work, conduct financial transactions, shop, access entertainment, and a myriad of other actions without location-based requirements.

Technology is permeated by people, government agencies and private sector companies. The more digitalization evolves, the more personal data, political documents and confidential business information are processed in an electronic format, and digitally transferred between locations. As the technology has allowed easier usage of services by, for example, creating the ability to work from remote locations, the technology has also generated a drawback in the form of cyber criminals.

Frauds, Identity- and Corporate Secret Thefts have been conducted before the invention of the Internet. However, they have increased explosively after the Internet became a general good according to Di Ciccio's (2014) research. Similar development was found in Tatham's (2018) research as well. Figure 1 below displays the identity

fraud complaint count development from 2001 to 2013, as discovered in Di Ciccio's research.

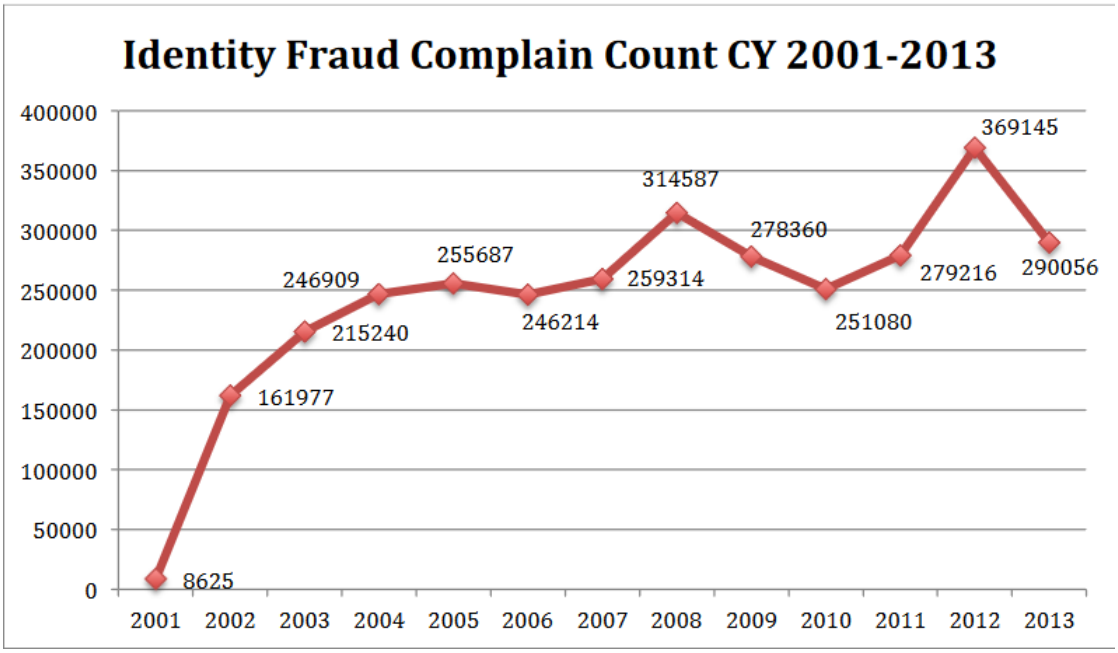


Figure 1. Identity Fraud complain count statistics from 2001 to 2013 (Di Ciccio, 2014)

One may ask – how are stolen data, frauds and other anomalies encountered in electronical platforms connected to cyber security training? This can be condensed to the expertise and capabilities of those dedicated to countering cyber-crime activities. As (especially) the financial and political stakes grow higher within the cyber security landscape, the robustness of the line of defence within the digital environment becomes ever more important, of which the skills of the employees are a significant component.

The monetary value of information has increased, and dedicated marketplaces have been established to trade personal information, confidential enterprise data and other commodities that different parties might use for their own benefit. These marketplaces include legal actors, such as Cambridge Analytica for advertising and marketing information, as well as black market actors operating within the TOR network, offering illegal services such as Distributed Denial of Service (DDoS) attacks. (Picchi 2018; Krebs 2016.)

Private sector entities, governments and national security agencies aim to prevent the anomalies brought about by increased cyberactivity, and the demand for cyber security training has grown as a consequence of attempting to ensure that these stakeholders have the expertise to combat modern cyber challenges. Computer science degrees generally contain some education regarding information and cyber security, however, the changing landscape calls for stronger and more specialized cyber security education.

2 Research purpose, methodology and scope

2.1 Purpose of the research

ISC^2 has reported that cyber security suffers a skill gap of approximately 500 000 employees in the United States. One of the key findings in the report mentions that the lack of skilled employees is the most common concern in responses conducted as a part of their research. (Strategies for Building and Growing Strong cybersecurity Teams: $(ISC)^2$ Cybersecurity Workforce Study 2019 2019, 8.)

The purpose of this research is to examine the current state of cyber security education in relation to stakeholder demands. This is achieved by attempting to answer the following questions:

- Does the current cyber security education fulfil the demands of different stakeholders?
- Do the stakeholder demands match the current curriculums of cyber security education?
- Can the contents of cyber security degrees at universities be improved to better meet the demand of stakeholders?

Several actions are taken to formulate answers to these questions. The first action is to compare different degree programmes and their structure to find out whether certain areas of knowledge or abilities are often omitted or skipped in the degree programmes. This creates an area of expertise currently demanded by stakeholders but not provided by degree programmes. Another action is to review stakeholder organizations and how different stakeholder cyber security personnel have reached their current position, as well as what related education the personnel have. Statisti-

cal prognosis about graduating students will be examined and compared to predictions of number of cyber security positions in the industry in 2022 to determine the existence and extent of an education cap in cyber security.

The hypothesis for the research is that by examining the current state of the cyber security education, the curriculums of the universities can be developed by comparing stakeholder demands to curriculum data and pinpointing missing areas of expertise demanded by stakeholders. This will allow for more uniform development of cyber security education in different countries.

This research will also provide basic information on aspects that are influencing cyber security training and encountered challenges. The research also includes future insights related to cyber security training.

This research is commissioned by JAMK University of Applied Sciences as a part of the CyberSec4EU project. The aim of the CyberSec4EU project is to act as a pilot project to create a cyber security competence network. In short, the project's goals include enhancing governance, closing of skill-gaps and developing and harmonizing cyber security capabilities of European countries. (About N.d.)

2.2 Research methods

The research method of this thesis is mixed method. Mixed method was chosen because the method allows for combining qualitative and quantitative data, as well as analyzing data collected between methods. (Shorten, & Smith; Saunders, Lewis, & Thornhill 2009, 152-155.)

The research approach for curriculum comparison is mainly deductive, and inductive in the stakeholder organization review. Deduction as a research approach is used to test a theory. Deduction requires a structured approach, and the data collected should be quantitative. The inductive approach allows to create a theory based on research data or patterns in the data, which is the opposite compared to the deductive research approach. (Blackstone 2012, 19-20; Saunders, Lewis, & Thornhill 2009, 124-128.)

Compared to deduction, the inductive approach is better suited to determine possible development ideas when developing cyber security education, as the inductive approach allows for generation of data without requiring strict structure or categorization of the data or possible answers.

2.3 Research problems and research data

The research data contains both quantitative and qualitative data. Most of the data is quantitative in nature, and has been collected to, for example, analyze the number of similar courses in different curriculums. Some qualitative data research data is also collected in the form of a questionnaire. (Steefkerk 2019.)

The research problems within this thesis are theoretical. However, if the research data is used to develop education and the curriculums of universities, the results answer a practical problem (McCombes 2019).

The data researched for the curriculum comparison is quantitative. The National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework is used to create a profile for the curriculums. The Cybersecurity Workforce Framework was picked as a baseline for categorizing individual courses within the curriculums, as this allows for the comparison of different approaches to cyber security education between universities. The weaknesses of the framework are discussed in Chapter 3.3.2.

The degree programmes in the comparison data included levels and a number of degrees shown in Table 1.

Table 1. Number of degrees per education level and continent

Continent and Level of education	**Number of degrees**
European Union graduate level	19
European Union undergraduate level	14
United States graduate level	21
United States undergraduate level	15
Total	**69**

A questionnaire was created to collect data regarding educational background of current cyber security experts, views on cyber security education and current stakeholder demands. The data was collected by interviewing people employed in a cyber security role across different organizations. The questionnaire received a total of 46 respondents, where two of the response data were dropped out as unsuitable. The query contains questions regarding background information in cyber security, industry and employment position, the extent of experience in cyber security, as well as open-ended questions regarding what the respondents perceive to be the shortcomings and skill gaps within the industry. Another straightforward approach to analyze the demands for cyber security experts in the field would have been the review of job openings and their educational and experience requirements. For this research, however, the direct interview path was taken instead, as job listings may not always reflect the true background of the person hired to that position.

Sampling method for the data collection follows the non-probability sampling method. The non-probability sampling method allows choosing the sample targets with certain criteria as determined by McCombes (2019), such as by requiring that the respondent works in cyber security industry or that the university provides cyber security education. The full questionnaire used to collect data from respondents is included in Appendix 1.

2.4 Scope

The research scope of the degree programme comparison is limited to comparing degree programmes organized in Europe and the United States of America. The research for stakeholder organization cyber security positions and the personnel's education in such positions, as well as the prediction of graduating future cyber security professionals, follows the same scope as the degree programme comparison. Only degree programmes active during Fall 2019 – Spring 2020 are included within the research data. The scope is extensive, as comparing just a few degree programmes would likely provide misleading results, as the chosen degree programmes might not reflect the real distribution of courses. Prediction of graduating future cyber security

professionals also requires large enough of a data pool to provide reliable results. In order to keep the theoretical background relevant to the current state of cyber security environment, the source materials for the theoretical portion of the research has been selected such that the publication date is in year 2010 or later, except in cases where the subject matter has not undergone significant changes since its publication.

The degree programme curriculum data is limited to course name, course description, credit counts in ECTS or CRH, as well as the role of the individual course within the curriculum (such as mandatory, elective or core). By limiting the scope of the degree programme curriculum data to these concepts, the analysis of the data becomes more straightforward and minimizes the probability of mistakes as the data is not too fine-grained. The curriculum data is categorized by using the Cybersecurity Workforce Framework as a baseline. The same baseline is used to analyze the collected questionnaire data to allow for comparison and contrast between the curriculum data and the questionnaire answers.

2.5 Research structure

The research has been structured such that it is as easy to understand and follow as possible.

The research begins with theoretical research into subject matters affecting cyber security and related education. The first sections of theoretical knowledge focus on reviewing aspects affecting cyber security and cyber security education in Chapter 3.1, as well as outlining challenges encountered in cyber security education of cyber security. Chapter 3.2 provides a closer view to education of cyber security, as well as educational structures and differences between the United States and the European Union. Chapter 3.3 reviews the available framework for measuring cyber security education and work and its utilization for curriculum comparison. Chapter 4 outlines data collection, unification and analysis methods. Data is summarized and analyzed in Chapter 5 to provide an answer to the research questions introduced in Chapter 2.1. Conclusions and findings of the research are discussed in Chapter 6, while suggestions for future research and development are included in Chapter 7. These progression of research through these stages is shown in Figure 2 below.

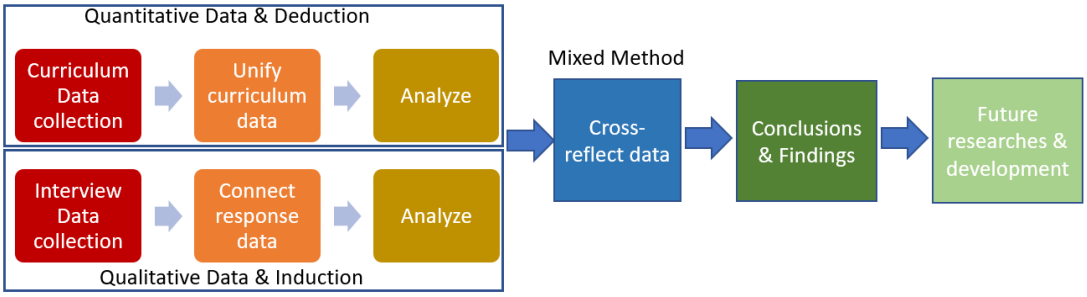


Figure 2. Research process structure

3 Theoretical Basis

3.1 Contemporary cyber security environment and demands from education

Cyber security is a constantly changing area of expertise. Trends in cyber security morph and form new paths without a pause, and some anomalies thought to be history may reapper at unexpected times. Gilles (2019) brings up how new threats and risks concerning cyber security emerge constantly, citing occurrences such as the poisoning of Artificial Intelligence -based defenses or breaking encryption with quantum computing, while the stakeholders attempt to find new ways to prevent these risks and threats from unfolding within their cyber space. (Sattler 2016; Top cybersecurity threats in 2020, N.d.)

Cyber security is often mistakenly mixed with the term “information security”, however, both of them overlap in certain ways (Buchy 2016). Kissel (2013) and Bhadauria (2016) define cyber security as protecting assets (such as servers or databases) contained within the organizations cyber domain, whereas information security is concerned with protecting information and data itself from unauthorized access, while ensuring data availability and integrity.

Improving the cyber security landscape for different stakeholders could technically be a fairly simple task, but in addition to technical implementation, other elements

and concepts have a play at security improvements as well. For example, legislation restricts the kind of data that can be monitored, politics can have an effect on how various cyber security solutions are implemented, and technical insularity can also play a role.

3.1.1 Governance and legislation

Governance and legislation have a significant impact on development of cyber security at the national level. In order to implement nationwide cyber security goals, proper governance and specific legislation is required to allow for effective implementation and ensure that governance goals are met. Different ramifications for violations are often added to legislation, such as financial sanctions, as is the case in European Union's directive in 2013 on cyber security and cybercrime (Directive 2013/40/EU). For stakeholders, following the legislation becomes a more attractive option than facing the consequences.

Legislations vary across different countries and states, and unfortunately, some countries currently have no form of legislation relating to cyber security (Cybercrime Legislation Worldwide 2020). As cybercrime is not bound within the borders of a country or a state, differing legislation between countries may cause challenges in solving criminal actions. This research creates an overview of governance and legislation, and how it might affect cyber security education within the territories limited by the scope.

One may now wonder, how do the legislation and governance aspects affect cyber security education? A person working within the cyber security field should be aware of different regulations governing the cyber security landscape, as this has a concrete impact on the person's work. People working for government agencies encounter different standards and requirements compared to a person who works at a private sector enterprise. For example, document classification is regulated in government agencies in Finland, whereas private sector enterprises are not bound to the same legislation (L 681/2010, $9).

In a hypothetical scenario, a private sector enterprise company owns affiliated companies in multiple countries, and the company's internal networks are connected to

each other. In this scenario, cyber security experts must be aware of legislation and their ramifications across multiple different countries. If an affiliated company is located in Afghanistan, the probability of solving local cybercrime cases is minimal, as the active legislation in Afghanistan does not recognize cybercrime as a crime, and holds no legislation regarding cyber security (Cybercrime Legislation Worldwide 2020). A cyber security expert working in public sector is unlikely to encounter a similar situation as the expert in this hypothetical scenario, however, it is important for both individuals to understand the aspect of risk management at least at a basic level.

In the United States, cyber security governance and legislation are roughly divided into two categories: federal and state specific regulations. Federal regulations apply to every state, and while the regulations themselves are usually not focused specifically at cyber security, they contain sections that touch on cyber security (Singh). An example of federal regulation is the Homeland Security Act from year 2002. The Homeland Security Act was implemented to protect the national security of the United States, however the regulation includes section called The Federal Information Security Modernization Act 2002, later referred to as FISMA, which holds a heavy focus on cyber security. FISMA requires government agencies to follow a framework managed and updated by National Institute of Standards and Technology (NIST). Contractors acting on behalf of federal agencies must also abide by the framework (Public Law 113-283-DEC. 18, 2014, $3551).

State specific regulations apply to the specific state at which the legislation is passed. An example of state specific regulation would be the California Security Breach Information Act, effective from July 2003. The regulation set mandatory processes for companies holding personal information of residents of California in case of security breaches or personal information disclosure, however the regulation only applies to stakeholders that have a physical establishment within the state. If a company that resides outside of the state of California has encountered a personal information disclosure that includes the personal information of a Californian resident, the company cannot be mandated to follow the processes enforced by the California Security Breach Information act. (CA Civ Code § 1798.29.)

Countries inside European Union face similar governance and legislations as the United States. However, there is a slight difference in governance and legislations, as the countries within European Union are autonomous. Processes to create regulations also differ by country, and these are not examined within this research as they are not of significant nature in relation to the research goals.

The similarity of governance and legislation between the United States and European Union follows the federal/state split of the United States. The regulations within European Union are either union-wide or country specific regulations. An example of a union-wide regulation is the General Data Protection Regulation (GDPR), effective from May 2018. The regulation enforces companies to abide by certain processes and definitions in situations where company processes personal information. This includes obligating the company to inform the people whose information was accessed within a data breach within 72 hours of the event (Regulation (EU) 2016/679, 52). As a union-wide regulation, GDPR is enforced at every member country of the European Union.

An example of country specific regulation is Latvian "Elektronisko dokumentu likums", effective from May 2004, last amended in June 2018. The regulation sets non-technical and technical specification requirements for electronical documents, signatures and signature-providers. As a nation-level regulation, the regulation is only enforced in Latvia (Elektronisko dokumentu likums*)*. Other European Union member countries may have similar regulations effective, though the specifics of the legislation vary across countries.

3.1.2 Politics and state relationships

Politics and political relationships play a role in development of cyber resiliency, as well as cyber security education. Cyber resiliency is defined as the ability to deliver and intended outcome continuously under any event within the cyber domain (Björck et al. 2015). Like regulations, the ability to understand how politics affect the risk management is required from cyber security professionals. Cyber security experts should be aware of the phenomena, risks and threats related to politics and state relationships. In some countries political decision-makers also control funding

of education, which directly impacts cyber security education in countries where the universities are government funded, such as Finland (HE 177/2016).

When examining countries and states in the world, all have one common object. The object is to protect the land, citizens and interests of the country or the state. States rely on either themselves or private sector companies to provide certain critical services to their citizens, such as electricity, public transportation and healthcare. States also provide security in the form of defense forces and laws. Development of the services provided by states has increased over time (Digitalisation N.d).

As mentioned in Chapter 1, many services that previously required a visit to the government office are now available remotely from home as a result of developments of information technology and networking. One may now wonder, who decides which technologies and fields to develop, and how? In democratic countries, a head of state and a parliament is selected by the means of an election. The elections can be assumed to be fair, and the head of state and parliament are chosen by voters.

In theory the process of democratic election is fair and the voters should be able to voice their opinion. However, the contest between political parties is rough. Information is valuable in the contest, and any information that cannot withstand daylight may be used as a weapon against opposition's political parties. This is also known as political influencing. Common phenomena in political influencing include disclosure of sensitive information, such as healthcare and criminal records of political candidates, fake news for disparagement of the candidate and denial of service against services provided by political party, such as websites. This is not only a domestic phenomenon, as it can be used to influence foreign states, as was the case in Trump Vs. Clinton elections in year 2016. This resulted in a more pro-Russia government in USA. (Abrams 2019.)

Relationships between different states and countries increases complexity of the cyber security. As mentioned in Chapter 3.1.2, countries provide services and protection to their citizens. As countries continue to provide and develop the services provided to their citizens, countries are also attaching their critical infrastructure, such as power plants to the global network. Critical infrastructure is always a prime target from a military point of view.

In a hypothetical conflict scenario between two nations, where the situation has escalated to physical contact, both parties have an interest towards disabling the opponent's critical infrastructures, such as power plants. The defending party has an interest to keep the power plant functional to continue providing electricity, whereas the attacking party has an interest to disable the power plant, disrupting the supply of electricity and regular actions of the enemy. As critical infrastructure is increasingly accessible from public network, cyberattacks can be utilized to target the power plant across borders.

A situation such as this has already occurred during the conflict between Ukraine and Russia, where Russian forces disrupted supply of electricity in Crimea in year 2015 (Nakashima 2017; Crashoverride: Analysis of the threat to electric grid operations, 10). Disrupting power supplies can cause major crises, such as power outages at hospitals and communication blackouts.

The cyber security aspect of inter-nation relationships also concerns political sanctions and product bans. An example of this includes the United States banning the use of products manufactured by Huawei, as well as the case where the United States demanded Adobe to stop providing their products for Venezuelan use. The reason for Huawei product ban was the accusation of using the products in espionage by the Chinese government (Mihalcik 2019; Keane & Reichert 2019). In the Venezuelan case, the sanctions held political reasons (Vol. 84, No.152 13884; Lee 2019).

Both cases show that state relationships and politics are important to include as a part of the risk management during cyber security planning and development phase. Politics and state relationships also affect technological choices in countries, increasing demand for expertise in specific manufacturer's products. This holds a direct relation to educational demands, as stakeholders may require expertise on the products that are manufactured by certain companies.

Inter-state relationships can also be beneficial between nations in the form of information trading and education. For example, NATO member nations share knowledge by conducting common cyber defense training (Training N.d). Sharing knowledge between participants increases cyber resiliency of the member countries, as well as tightens the skill gap and strengthens the entire organization.

3.1.3 Stakeholders

Technological development and stakeholders demand for expertise in the cyber security has a wide effect on cyber security education. The demand for knowledge, skills, and ability to use up-to-date technologies and methods is increasing, mostly due fast technological development and changing nature of threats that stakeholders encounter in cyber domain.

Cyber security stakeholders can be divided into two categories: private sector and governmental stakeholders. According to Russel (2002), most of the technological development takes place in the private sector. The reason for this is in the nature of the corporations in private sector, where the main goal of the corporation is to gain maximum financial benefit from the business, which allows for more finance to be spent in the development of the products and business. Governmental agencies also have cyber security related development; however, the budget is gathered from limited state tax income.

Development targets are also often related to the interest of the stakeholders. Private sector products and services are often developed to enhance sales, while governmental development is related to goals set by the state, such as secure services provided to citizens, enhancing cyber resilience or even cyber warfare.

Abilities, skills, and knowledge demanded by the stakeholders overlap with each other, as many cyber security related assets such as firewalls are used in both the private and governmental sector. However, depending on the stakeholder, certain capabilities are not necessary. For example, Das and de Guise (2019, 150) observed that many government agencies avoid using public cloud infrastructure due to threats and risk management, mitigating chances that sensitive governmental data is disclosed. Meanwhile, the private sector is beginning to embrace public cloud infrastructures, so the demand for security experts with cloud infrastructure specialization is high. The differences in demand of desired skills sets challenges to the universities when developing curriculums to meet the demands of the stakeholders.

3.1.4 The challenges for universities

Chapters 3.1.1-3.1.3 examined the different factors affecting cyber security education. Funding mechanisms of universities, inter-nation relationships, stakeholder expectations and a myriad of other factors create challenges for universities and their graduating students.

Funding mechanisms differ between universities. Many of the universities collect tuition fees from their students, while some universities are funded mostly by the government through taxation. The location of the university often affects the tuition fee, and in some cases other qualifying terms affect the tuition fee, such as the student's income for tuition in Italian universities (Compare tuition fees schemes in Europe N.d). As a comparison, most of the Finnish universities do not collect a tuition fee from EU citizens or exchange students (HE 77/2015). Universities funded by taxes receive their funding from the government, which often contains specific requirements or objectives. For example, Finnish universities receive a major share of their funding for every graduating student (Korkeakouluille uusi rahoitusmalli 2019).

While not immediately apparent, the funding of universities can have an impact on cyber security education. Tuition fees can be linked with the behavior of the students. Students admitted to universities without tuition fees are more motivated when compared to commercialized universities, where the only qualification for admittance might be the ability to pay (Kuronen, & Mansikkamäki 2017, 27). As a researcher's note, there is a slight paradox with this claim, as Universities with tax funding and specifically funding objectives concerning the number of graduating students may be motivated to allow students to graduate with lower standards due to the funding method.

Another challenge for universities is technological modernization. Universities that have surplus funding can include more modern platforms and technologies within the curriculum, whereas universities struggling with the budget might have to continue teaching old technology platforms to their students as upgrades are beyond their budget.

Even though the baseline in the technologies is often the same, in a hypothetical situation where two students are securing an identical laboratory environment with a

different version of certain technology (such as Windows Server 2016 versus Windows Server 2019), it is more likely that the student working with a more modern environment will have the ability and training to harden the environment to a greater extent due to more enhanced security and security capabilities in Windows Server 2019 (Compare features in Windows Server versions: View the new hybrid,security, and application platgorm features of Windows Server 2019 as compared to previous versions N.d*)*.

Relationships between countries influence cyber security education in terms of the strategic autonomy that different countries want to protect (Rethinking Strategic Autonomy in the Digital Age 2019, 2). A direct impact of this influence includes aspects such as choice of technology. As countries can determine their choices of technologies and manufacturers due autonomy in governmental agencies, this can cause cross-state mismatch in technological expertise in educations. However, many of the technologies are technically similar to each other, such as firewalls, and knowledge gained in one subset of technology can be directly applied to a different area of technology without too much of a challenge. The challenge posed by the differences is still worthy of note. Indirect impacts include aspects such as cyber resilience related state secrets which countries do not want to disclose to other countries. Some countries might have more sophisticated technological solutions or methods for cyber intelligence or other tasks, which are never disclosed to other countries (Bing, & Schectman 2019). While the disclosure could improve cyber resiliency of other countries, the disclosure could simultaneously lower the cyber resiliency of the disclosing state, as the information or methods used in the disclosed state would no longer remain a secret and would provide critical information for the nation's adversaries.

Another challenge in cyber security education is meeting expectations of the education from different stakeholders. As mentioned in Chapter 3.1.3, stakeholders often expect up-to-date expertise on technologies, and the demand for desired skills depends on stakeholders. ISC^2 Reported that the cybersecurity workforce gap was almost 500 000 positions in the United States. Additionally, Oltsik's (2019) research indicated that the skill gap between applicants and the stakeholders is increasing (Strategies for Building and Growing Strong cybersecurity Teams: $(ISC)^2$ Cybersecurity Workforce Study 2019 2019, 8).

A significant challenge concerns what universities should teach to their students to answer the demands of stakeholders. As cyber security is a constantly evolving area of expertise and the trends in cyber security related anomalies change constantly, the curriculum would require constant updating to answer the challenge. Constant updates or changes to the curriculum would create a challenge in determining which skills, abilities or knowledge should receive less attention to create room for teaching the new trends or technologies.

Currently most of the cyber security degrees are formed with a combination of mandatory and elective courses, and the baseline of the curriculum should be same for all students with elective courses so that the students can specialize in areas of expertise that they are interested in. No research into this subject matter was found, but the structure of the curriculums and increasing skill gap may indicate that the students play a part in creating the skill gaps themselves, as universities leave the responsibility of degree composition to their students in the form of a significant portion of elective courses.

3.2 State of contemporary cyber security education

Cyber security education is available in multiple educational levels, with certain countries providing voluntary courses aimed at larger audiences, from children to elders. Education for citizens is often provided by governmental agencies in multiple educational formats such as courses and gamification platforms. In addition to publicly provided courses and prior education, stakeholders tend to have their own internal courses related to cyber and information security to increase workforce competence and protect assets of the stakeholder. (Lehto, & Niemelä 2019, 20.)

3.2.1 Educational levels

Cyber security education is divided into two different educational methods, when comparing educational stages of undergraduate degrees or higher education. The first method is a cyber security based degree programme, where the degree programme objective is to produce in-depth specialists within cyber security area of expertise. Another method is including cyber security studies in degree programmes

not majoring in cyber security, such as degree programme of software development. (Lehto, & Niemelä 2019.)

While cyber security studies included in degree programmes majoring in another field are usually a surface scratch of the subject, these studies are important for creating a base level understanding of the field, such as country wide cyber security awareness.

In addition to degree programmes, cyber security education is provided in vocational level education and community colleges. Usually the depth of the studies is very limited and concerns only the very basics of the security, such as how to update the operating system or how to install end-point protection products. These educational levels are not included in the target scope of the research but are worth a mention.

Additionally, cyber security specialization education is available in some universities. These specialization educations do not tend to grant a degree title to a graduating student.

3.2.2 Education structure

Based on the collected course data, most of the undergraduate curriculums are composed of courses of three or four different types. The types of courses in an undergraduate program typically include Common Basic (CB) studies, Specialization (S) , Specialization Elective (S/E) studies and Elective (E) studies.

Common Basic studies are usually general courses mandatory for every student in the university, such as courses focused on research and writing. Courses that are mandatory within a certain faculty are included in Specialization studies, such as computer fundamentals for information technology faculties. Studies included in Specialization/Elective studies are often the courses that are included in modules directing the student's specialization in certain field of expertise. As an example, a cyber security student could specialize in Digital Forensics and Incident Response, whereas another student could specialize in Penetration Testing. Elective studies usually allow student to choose studies from a pool of available courses, allowing the student to direct the curriculum towards their interests. The classification of course

types are a result of the researcher's observations, and these may vary slightly across universities.

Degree programme curriculums typically also include internship and a thesis or capstone course, which could be counted among specialization studies as they focus on improving the student's skillset within a specific subset of their specialization.

In most graduate level degree programmes, the course types are limited to Specialization and Elective studies. As in undergraduate curriculums, the graduate degree often includes a thesis or capstone course depending on the university where the studies are performed.

3.2.3 Differences between the United States and European Union

Comparing education in the United States and European Union shows that many overlapping similarities as well as vast differences exist. The credit system is different; The United States uses Credit Hours (CRH), whereas European Union uses a unified European Credit Transfer and Accumulation System (ECTS). One Credit Hour in the United States is approximately equivalent to two ECTS credits (Weingarten 2020).

Similarities can be found in the structure of degree programmes, as the same elements can be found on both: basic studies, elective studies and professional studies. Weight given to each type of course varies across universities. For example, the amount of elective studies required for a Master's degree in Cyber Security at University of Tampa totals 16 ECTS credits, whereas in JAMK University of Applied Science the required amount for elective courses is five ECTS.

Based on observation on collected curriculum data, tuition fees for every student are a standard occurrence in the United States based universities, whereas in European Union some universities allow European Union citizens to educate themselves for free, while collecting tuition fees from non-European Union citizens.

3.2.4 Cyber security educational split

Cyber security education can be split in two main categories: management and technical. Management-based studies provide students with the ability to create processes, evaluate risks and threats that an organization might encounter, and define

how cyber security is managed in organizations. Technical studies include more detailed studies on hands-on implementation of technologies, such as configuring firewalls, Public Key Infrastructure or how to perform vulnerability scanning.

3.3 Frameworks for measuring skills in cyber security

As a cyber security education specific framework does not exist at the time of writing, a more general framework is used instead. The United States based National Institute of Standards and Technology (NIST) has created a National Initiative for Cybersecurity Education (NICE) with several different goals, including developing learning, education and skills in cyber security alongside enhancing career development (The National Cybersecurity Workforce Framework 2017, IV). NICE has published a Cyber Security Workforce Framework (NCWF), created to provide a tool to categorize and describe different cyber security work tasks. Even though this framework was not directly created as education framework, the framework can be used to identify, categorize, and determine the contents within cyber security degree's curriculum. The framework disassembles cyber security work roles and lists the features in the role, including the following information: Work Role Name, Work Role ID, Category, Specialty Area, Work Role Description, Tasks, Knowledge, Skills and Abilities (The National Cybersecurity Workforce Framework 2017, 95).

3.3.1 NCWF Work Role description

Individual work roles described within the NCWF provide a detailed basis for categorization of skills. Work Role Name and Work Role ID contain the name of the role and the role's unique identifier. Based on observation when collecting data, the Work Role ID is at times referred to in job advertisements; however, this practice seems to be more of an exception than a rule. The Work Role ID is composed of the framework's Category and Specialty Area, which helps in immediately identifying the nature of the work.

Categories are split to seven different categories: Securely Provision (SP), Operate and Maintain (OM), Oversee and Govern (OV), Protect and Defend (PR), Analyze (AN), Collect and Operate (CO) and Investigate (IN). Categories broadly describe the nature of the cyber security work in each category. For example, when completing

work within the category “Analyze”, the person “performs highly-specialized review and evaluation of incoming cyber security information to determine its usefulness for intelligence” (The National Cybersecurity Workforce Framework 2017, 11*).*

Category contains multiple Specialty areas specific to that to that Category, such as Exploitation Analysis. The framework currently contains a total of 32 different Specialty Areas and descriptions for each. (The National Cybersecurity Workforce Framework 2017, 12-23.)

Work Role Description describes the Work Roles under a Specialty Area, which, for example for Exploitation Analysis, contains the following information:

> *Collaborates to identify access and collection gaps that can be satisfied through cyber collection and/or preparation activities. Leverages all authorized resources and analytic techniques to penetrate targeted networks.* (The National Cybersecurity Workforce Framework 2017, 20.)

Each Work Role under Specialty Areas receive a running Work Role ID identifier which completes the Work Role ID. Exploitation Analyst of the previous example has a Work Role ID of AN-EXP-001. With the Work Role ID, employees and employers could easily refer to the specific demands imposed by the job.

The framework also includes practical work descriptions, as well as tasks, knowledge, skills and abilities attributed to the Work Role which the person is expected to fulfill to successfully work the Work Role.

The framework currently contains 1007 different tasks, 630 knowledge items, 374 skills and 176 abilities. Like work roles, each item has a unique identifier. For example, Task T0868 is described as “Work with business teams and senior management to ensure awareness of “best practices” on privacy and data security issues” (The National Cybersecurity Workforce Framework 2017, 53). Knowledge, Skill and Ability items hold similar descriptions. Each of the work descriptions can contain multiple items from each of the categories. Figure 3 displays the complete Work Role Description for Cyber Defense Analyst, including the plaintext description in addition to listing of associated individual Tasks, Knowledge, Skills and Abilities. (The National Cybersecurity Workforce Framework 2017.)

Work Role Name	Cyber Defense Analyst
Work Role ID	PR-CDA-001
Specialty Area	Cyber Defense Analysis (CDA)
Category	Protect and Defend (PR)
Work Role Description	Uses data collected from a variety of cyber defense tools (e.g., IDS alerts, firewalls, network traffic logs.) to analyze events that occur within their environments for the purposes of mitigating threats.
Tasks	T0020, T0023, T0043, T0088, T0155, T0164, T0166, T0178, T0187, T0198, T0214, T0258, T0259, T0260, T0290, T0291, T0292, T0293, T0294, T0295, T0296, T0297, T0298, T0299, T0310, T0332, T0469, T0470, T0475, T0503, T0504, T0526, T0545, T0548
Knowledge	K0001, K0002, K0003, K0004, K0005, K0006, K0007, K0013, K0015, K0018, K0019, K0024, K0033, K0040, K0042, K0044, K0046, K0049, K0056, K0058, K0059, K0060, K0061, K0065, K0070, K0074, K0075, K0093, K0098, K0104, K0106, K0107, K0110, K0111, K0112, K0113, K0116, K0139, K0142, K0143, K0157, K0160, K0161, K0162, K0167, K0168, K0177, K0179, K0180, K0190, K0191, K0192, K0203, K0221, K0222, K0260, K0261, K0262, K0290, K0297, K0300, K0301, K0303, K0318, K0322, K0324, K0332, K0339, K0342, K0624
Skills	S0020, S0025, S0027, S0036, S0054, S0057, S0063, S0078, S0096, S0147, S0156, S0167, S0169, S0367, S0370
Abilities	A0010, A0015, A0066, A0123, A0128, A0159

Figure 3. Example of Work Role Description in NCWF framework (The National Cybersecurity Workforce Framework 2017, 110).

Although the framework is targeted more towards labor market purposes, the framework can be utilized to determine contents and expected results of course curriculums in an educational context. Students could also use the framework as a guide to professional development to determine their abilities and capability to fulfill demands of job based on their description, and additionally identify knowledge, skills and abilities that need development to be able to work a specific role.

Like any framework, NCWF has its pros and cons. A major positive aspect of the framework concerns scaling, as the frameworks suits organizations of various sizes, from small to large. The framework is also thorough, containing most of the cyber security related work titles described.

However, the usage of the framework seems to be limited mostly to the United States, and no competing or alternate framework is available. Also, at the end of the day, stakeholders still determine their own demands when it comes to different work roles. For example, Cyber Operators in two different companies may in reality have different responsibilities even within the same tasks – one Cyber Operator may be required to collect and analyze log files themselves, while another Cyber Operator

might be limited to forwarding the necessary logs to another escalation point. Despite of the cons, the framework is suitable for evaluating the contents of curriculums and will be used during this research, as the cons mostly consist of labor side evaluation.

3.3.2 Utilizing the framework

The NICE Cyber Security Workforce Framework is utilized in the research by matching the courses in university curriculums to main categories of the framework. The courses are classified according to main categories of the framework, and a profile of the curriculum is created based on the classifications. After the creation of the profiles from curriculums, a profile from the stakeholder demands is generated and compared to the curriculum profiles. The classification could be even more detailed and combining the classifications, it would be possible to create profiles, which NCWF work roles could be filled with each of the curriculums. However, this is out of the research scope, and would require own research from the topic.

4 Measurement of cyber security education availability and requirements

4.1 Curriculum comparison

Curriculum comparison is conducted by collecting courses included in graduate and undergraduate degrees related to cyber security, such as Bachelor of Science in Cyber Security, or Bachelor of Science in Digital Forensics (as digital forensics can be classified as a subcategory of cyber security). Selection of universities was conducted by arbitrarily selecting 21 graduate degrees from the United States and 19 graduate degrees from European Union, and 15 undergraduate degrees from the United States and 14 from European Union. No differentiation has been made between degrees requiring full-time attendance and degrees consisting partly or completely of online studies.

4.1.1 Collected research data

Data collected from the universities and the purpose of the collected information is presented in Table 2.

Table 2. Collected curriculum information and purpose

Collected information	**Purpose of the information**
Course name	Used in within research as the main key when comparing curriculum courses and stakeholder demands. Sum of credit hours is used for creation of curriculum profiles from the different universities.
Course ID	Included in the data to enable later use of the collected data for future re-search.
Tuition fees	If available, a comparison between price per credit can be conducted between continents.
Course description	If available to support possible future research purposes.
Sum of course credits	Sum of course credits across all courses are mapped to a radar graph with dif-ferent NCWF categories to represent each axis.
Course type	Role of the course within the degree. Course types are split into the following: Common Basic (CB), Specialization (S), Specialization/Elective (S/E) and Elective (E). CB and S are mandatory for the de-gree, S/E courses are part of a module selected by a student as a part of their

	degree, with the expectation that student will complete one or more complete modules to complete the degree. E courses are purely optional; however, a set number of elective courses are usually required within a degree.

As most of the curriculums contain at least ten or more courses and manual analysis would consume a significant amount of time, data analysis is performed in software specialized in analyzing a large quantity of data. The collected data was transformed to a standardized form in spreadsheets and subsequently uploaded to a Splunk server. Splunk is a big data search-and-analyze engine developed by Splunk Inc. The data was imported to four different indexes: Bachelor EU, Bachelor USA, Master EU, Master USA. The split indexing enables easier comparison of differences in curriculums between continents. Aggregation of data is also possible by combining the results of different indexes.

4.1.2 Categorization of degree programmes

The degree credit hour counts vary between 60 ECTS to over 120 ECTS in graduate programs and between 168 ECTS to 240 ECTS in undergraduate programs, so the degrees are also categorized based on credit hour count when comparing the results. The categorization groups consist of degree programmes with credit hour count of 60 to 85 ECTS, 86 to 110 ECTS and 111 to 130 ECTS in graduate level, and 160 to 190 ECTS, 191 to 220 ECTS and 221 to 240 ECTS for undergraduate level. An overall comparison is also conducted for all the degree programmes regardless of the credit hour count of the programme.

4.1.3 Categorization of courses

Categorization of courses is done by comparing the course to the NICE Cyber Workforce Framework's Categories. Categorization is primarily based on course name, and if the course name is undescriptive, course description is used if available. If the

course could fit into multiple categories, the course is added to the two most significant categories. Some courses included elements from more than two categories, but only the two most prominent categories were chosen to keep the categorization simple.

Courses included general studies from information technology aspects unrelated to cyber security, such as programming in single programming language or operating system configuration. In such cases, the course was added to the category closest related to cyber security, for example programming courses were added in “Secure Provision” category, which includes software development as Specialty Area. The courses not applicable to any category were categorized to “unrelated” category – these included courses such as different language courses. The unrelated category also includes a few information technologies courses, such as generic information technology project courses, for example, Linnaeus University’s Project Course in Computer Science. For a specific list of categorizations, see Appendix 2. The appendix includes the main categories of the framework and areas of studies included under each category.

4.2 Questionnaire for stakeholders

To answer the research question “does the cyber security education answer to the stakeholder demands”, a questionnaire was created to provide data from the viewpoint of different stakeholders. The data collected with the questionnaire allows for comparison of collected course data against the stakeholder demands. The questionnaire included questions for collecting background information, such as how long the respondent has worked in information technology field, or which industry they work in. Survey respondents were chosen arbitrarily within the cyber security field of work. The respondents were not split to continent categories as was the case with curriculum data.

Most of the answer fields were left as free text fields to gather qualitative data instead of quantitative. This was intentional, as creating the questionnaire with pre-defined answers could channel the answers towards pre-selected topics, and the real demands could remain unveiled. The data was analysed and answers categorized to

similar topics. For example, answers concerning programming and scripting are combined under programming topic.

The combined data and categorization lists are available in Appendices 3-8. The raw questionnaire response data is available as a separate file, as detailed by Appendix 14.

4.3 Expertise profiles of degree programmes and stakeholder demands

To express curriculum weighting in NCWF categorization, a radar chart is made for each continent & degree level. The radar charts are generated based on the length of the degree programme in ECTS. The classification for different length of curriculums was determined in Chapter 3.2.1. The formula for the radar chart is course length in ECTS added to NCWF categorization. For Stakeholder demands, the radar charts are generated by response counts added to NCWF categorization. The responses were categorized to NCWF in accordance with the Appendices 2-7.

5 Measurement results

5.1 Questionnaire results

The questionnaire received a total of 46 responses. Two of the responses were removed from the answers as the data contained in answers indicated that the responses were deliberately misleading, leaving a total of 44 responses. When creating statistics from the collected data, the following rules were used: all options that were mentioned five or more times within the responses were included in comparison charts, but if none of the options had five responses or more, five most answered options were included in comparison. These rules were not applied to background data. The combined response data can be found in Appendix 13. The Raw data is provided in Appendix 14.

Background data is be used to create a profile from the work force that has replied to the questionnaire. The profile is not directly used in this research, but if similar research is created, the profiles of the respondents could be compared to give review if the responses vary between the profiles.

The professional cyber security profile of questionnaire respondents varied significantly, with respondents included from multiple industries and organizational positions, from SOC Agents to Chief Information Security Officer. The variation in respondents' experience provided insights from many aspects of the stakeholders, from cyber security experts early in their career all the way to the veterans who have worked in the field for decades.

5.1.1 Respondents' industry of employment

Industry data was collected as background information on which industry the respondents are employed at. Respondent data was merged into general categories to allow for a clearer image of the distribution of industry. For example, ICT and Telecommunications were merged, as many of the companies in Telecommunication industry provide ICT services in addition to Telecommunication services. According to collected data, vast majority (64%) of the 44 respondents work in ICT and Telecommunication industry with Health Care and Pharmaceutical industry being the next most common industry, details shown in Figure 4.

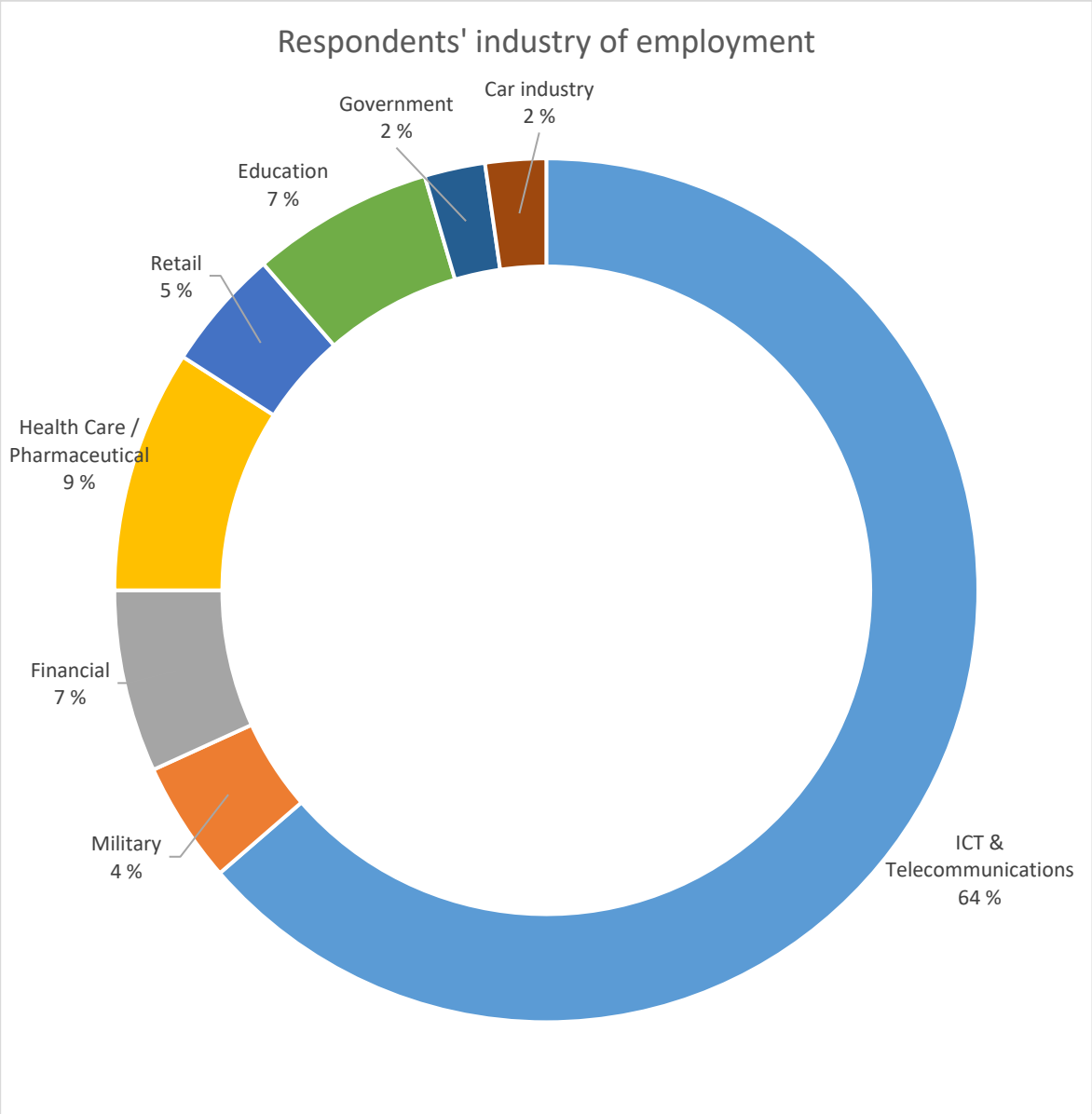


Figure 4: Employment industry distribution of respondents

5.1.2 Public-private sector distribution of respondents

Like Industry data, the Sector distribution data was collected as background information to provide insight into sector distribution in cyber security work. Majority of the 44 respondents worked in private sector, as depicted in Figure 5.

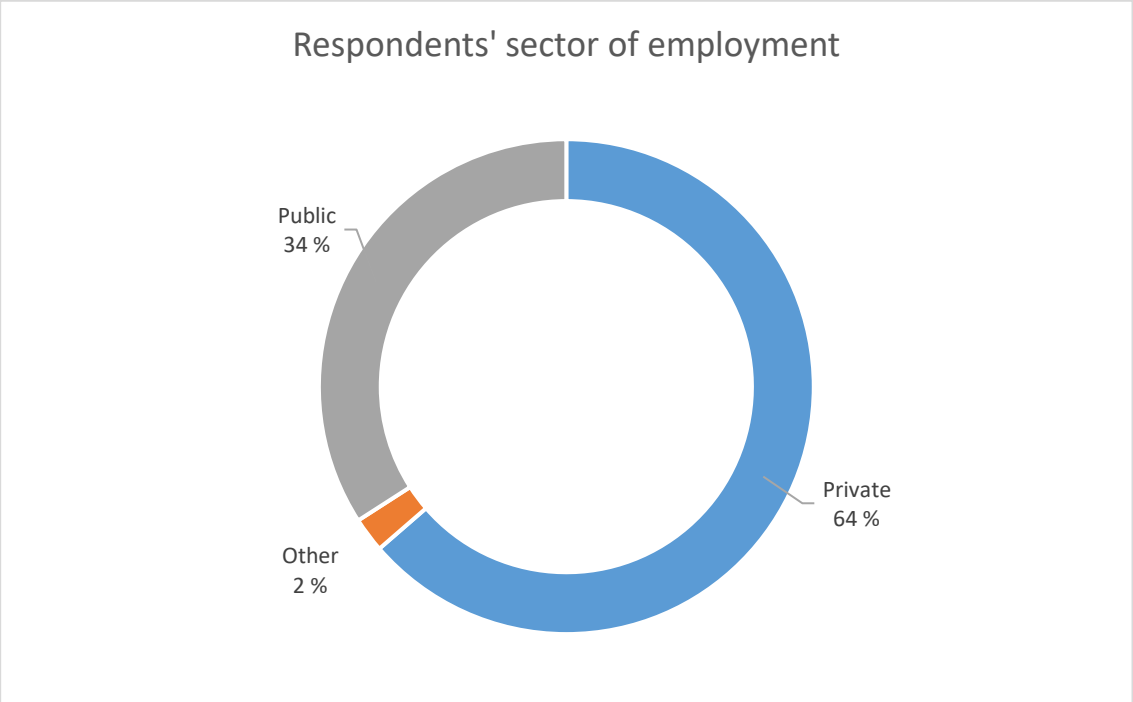


Figure 5: Employment sector distribution of respondents

5.1.3 Respondent job titles

Questionnaire responses for different job titles are distributed as shown in Figure 6 below. In order to simplify the chart presentation, titles were combined from categories that consist of similar roles, for example manager positions containing titles such as Red Team Manager and Director of Technology. A total of 44 responses were received for this question, with the two largest emerging job titles being a specialist (consisting of Specialist, Analyst, Engineer, Consultant, at a total of 45% of respondents) or a manager (at 32% of respondents).

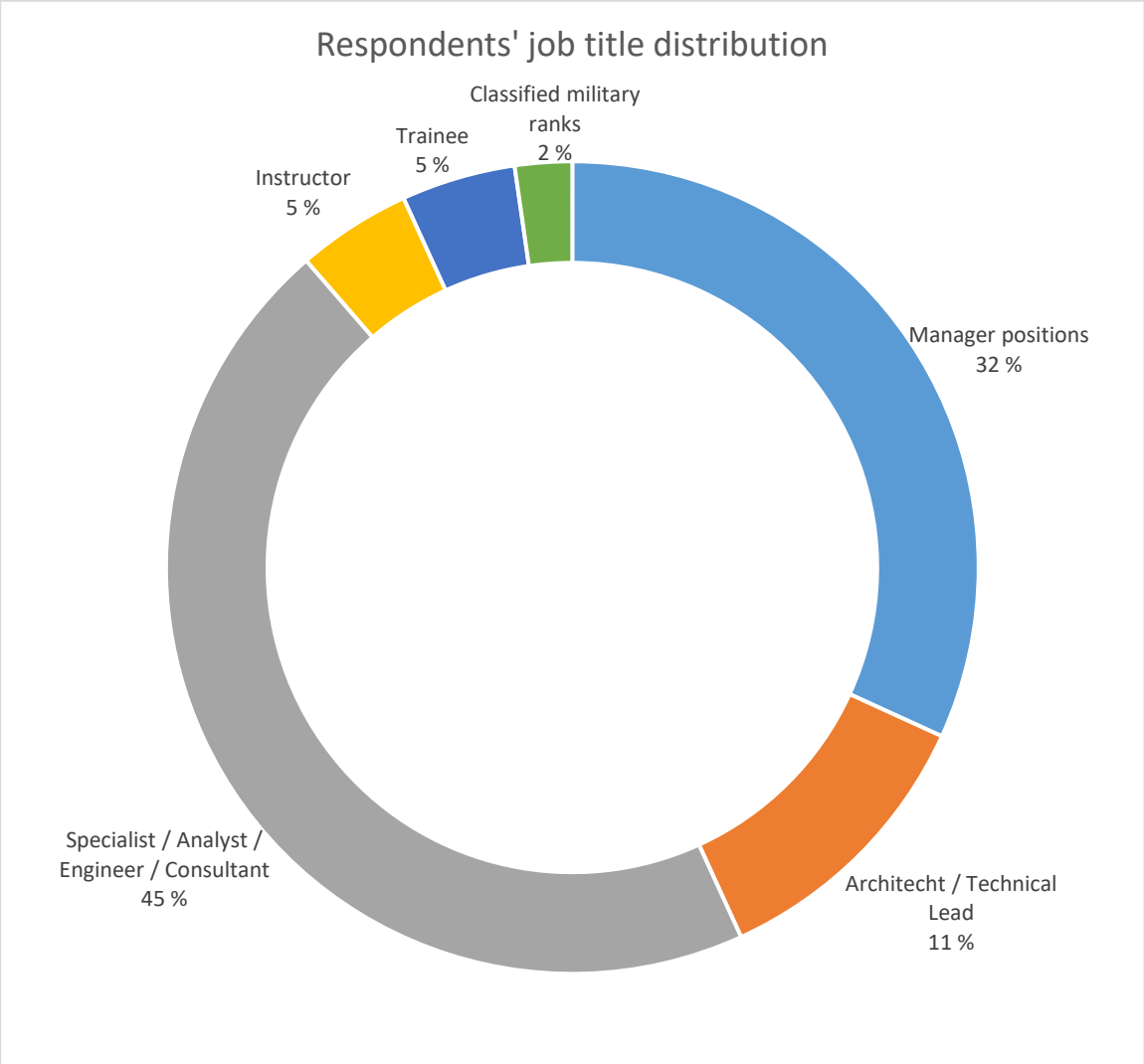


Figure 6: Distribution of respondent job titles

5.1.4 Education level of respondents

Respondents were asked for their education level and degree. If the respondent had multiple degrees mentioned in their response, all degrees were counted towards the statistics. ICT-related educations were categorized into cyber security and non-cyber security degrees in order to indicate the difference in distribution of direct cyber security degrees and other ICT-degrees. Based on the response data, landing a cyber security job does not necessarily require an ICT-related degree. However, majority of the 44 respondents had either non-cyber security ICT or cyber security related education.

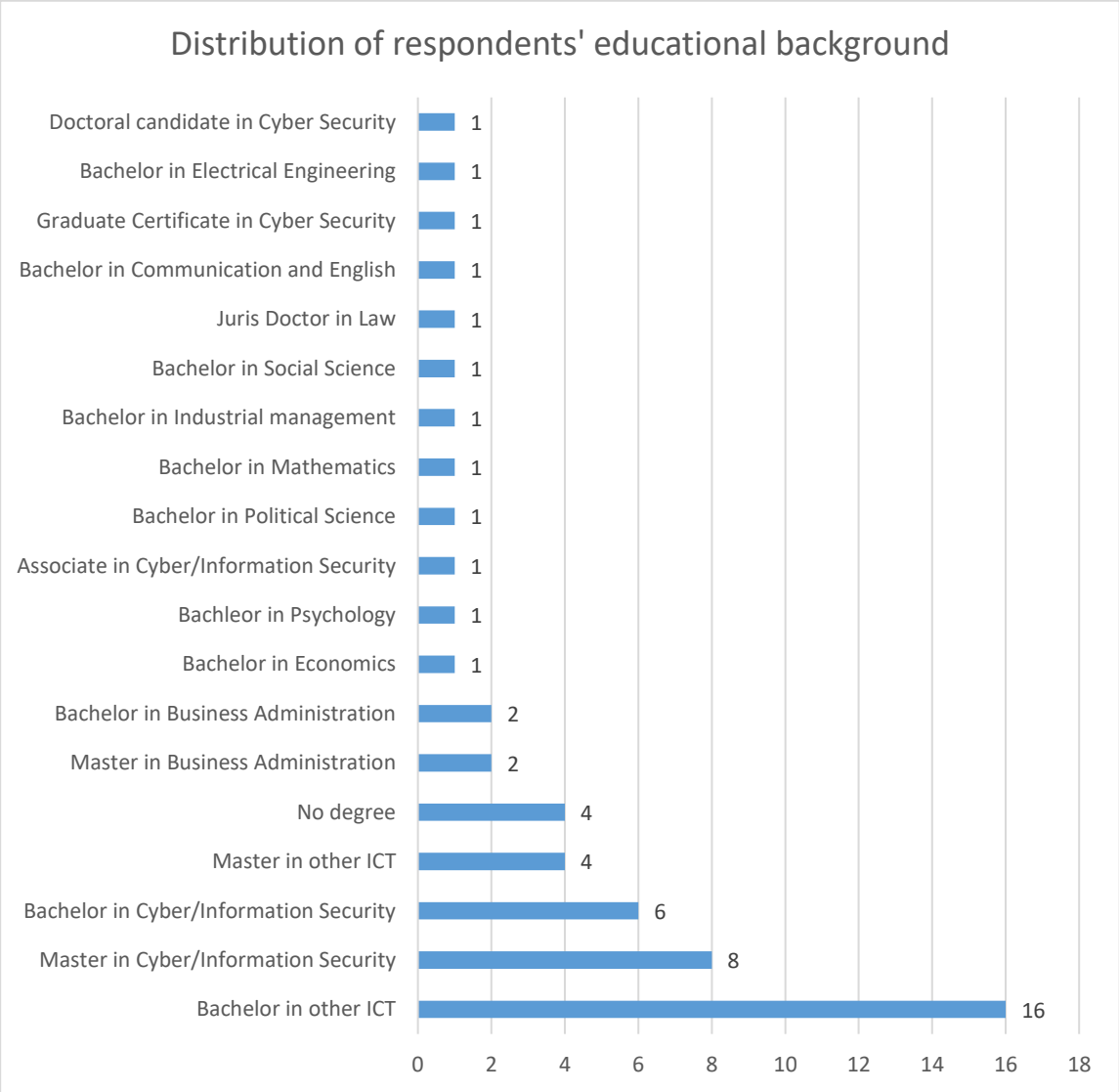


Figure 7: Distribution of respondents' educational background

5.1.5 Non-degree Cyber Security related education

Respondents were also asked if they have educated themselves with non-degree education related to cyber security, such as certificates, cyber security related courses or hobbies and events. As shown in Figure 8, almost all of the respondents had some additional non-degree education related to cyber security. The question had 41 answers, indicating that three of the respondents had not obtained any additional education.

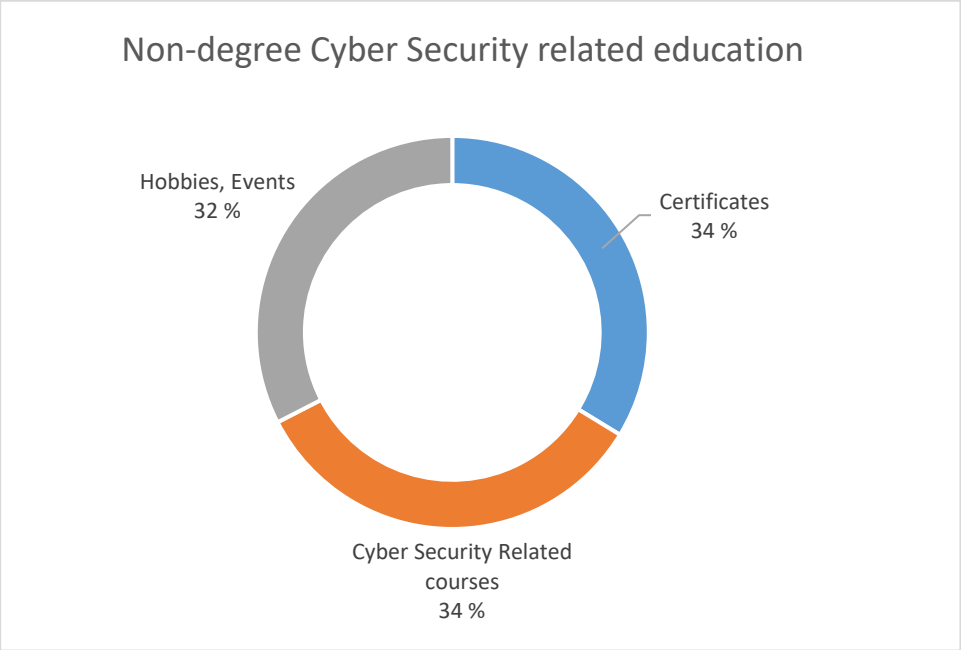


Figure 8: Non-degree related cyber security education among respondents

5.1.6 Distribution in technical and management aspects of cyber security

Respondents were asked regarding the distribution of work in technical and management aspects. In larger corporations the technical and management roles often tend to be clearer, however, smaller corporations may only have a few employers working within the cyber security organization, which is more likely to result in the same person acting in managemental and technical roles. The distribution of management and technical balance of the 44 respondents is portrayed in Figure 9. Technical and management aspects are highly polarized, with a handful of respondents working in hybrid roles.

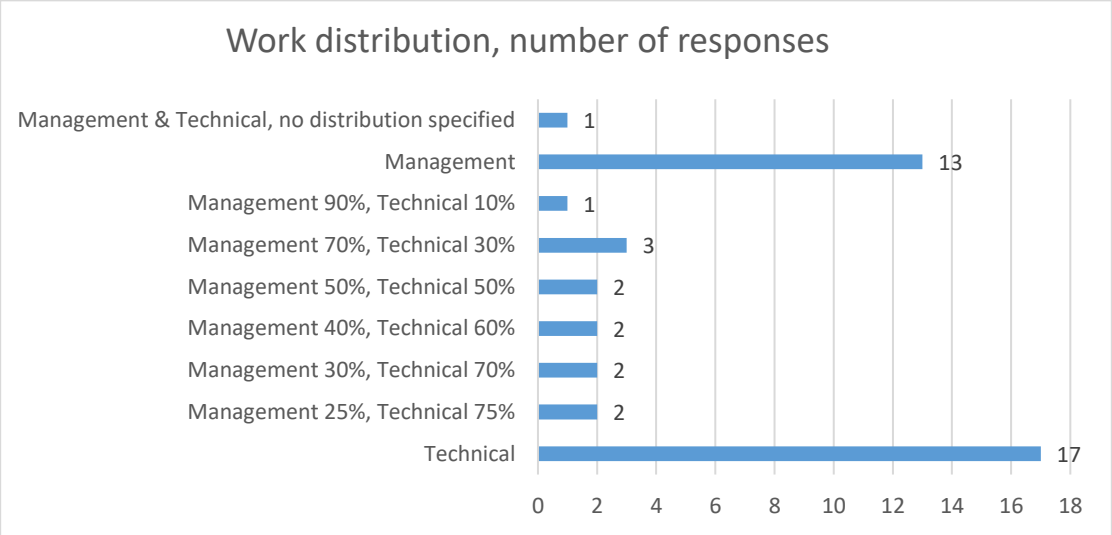


Figure 9: Distribution of respondents' work between technical and management aspects

5.1.7 Respondents' career duration in cyber security & ICT

Respondents were asked how many years they have worked in cyber security. Figure 10 shows that, of the 44 respondents, ten respondents have worked over ten years in cyber security, nine respondents between five to ten years, 12 respondents between two to five years and 13 respondents between zero to two years.

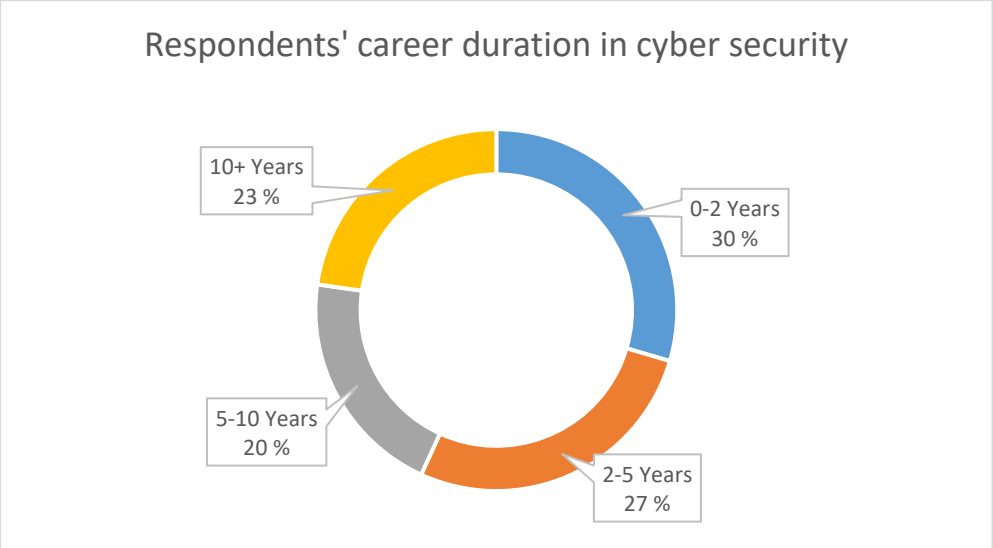


Figure 10: Respondents' career duration in cyber security

Respondents were also asked how long they have worked overall in ICT, and with same years of experience scope expressed in figure 11, it could be concluded that respondents have several years of other ICT experience before moving to cyber security, as the experience range in years scale for 75% of respondents to five to ten years or more.

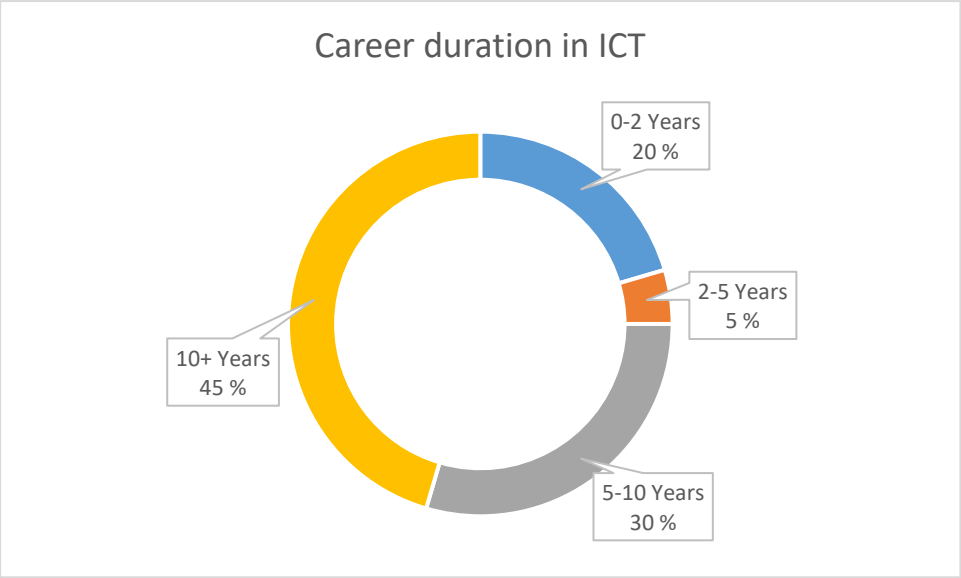


Figure 11: Respondents' career duration in ICT

5.1.8 Most important areas of expertise according to respondents

Respondents were asked to name three to five areas of expertise which the respondents felt to be the most important areas of expertise to have to properly work in Cyber Security. Answers were consolidated under categories to provide a higher level perspective to the results. Item categories with more than 5 answers per category were included in statistics. According to response data, 20 out of 44 respondents ranked soft skills as one of the most important areas of expertise, shown in Figure 12. Rest of the responses consisted of more technical aspects of ICT, such as networking and programming.

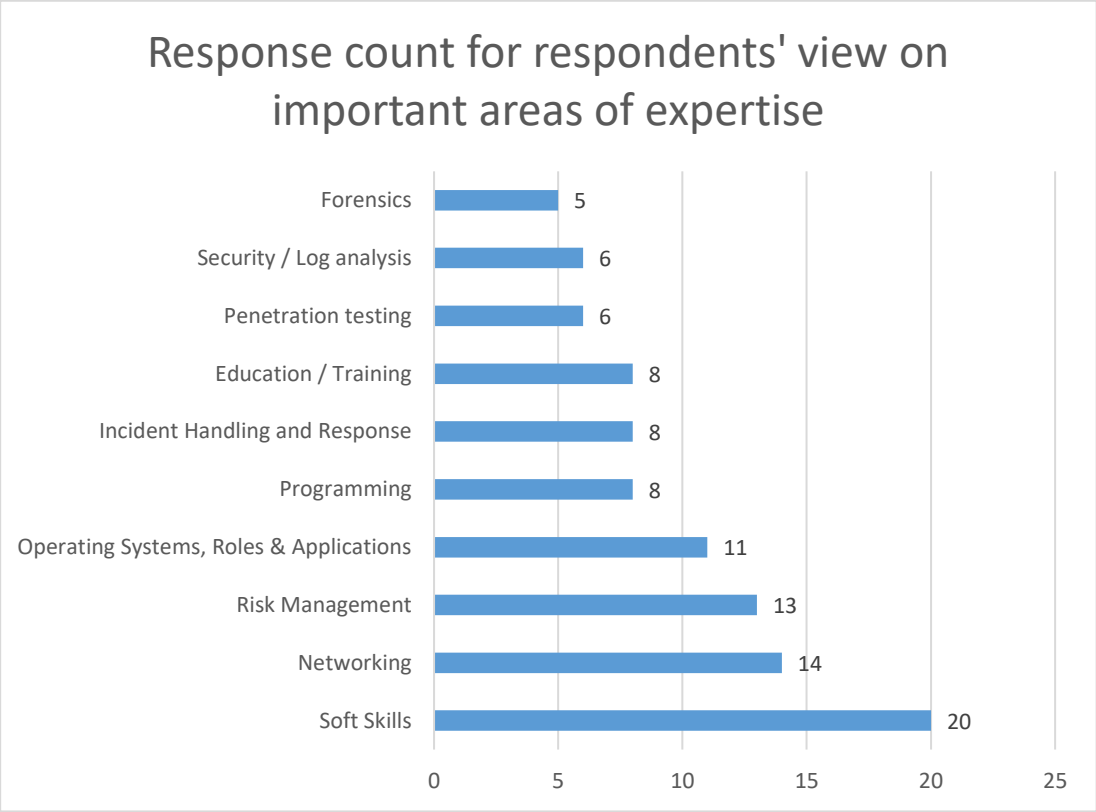


Figure 12: Respondents' views on important areas of expertise

5.1.9 Respondents' view on expertise to be improved

Respondents were asked to name skills in three areas of expertise that they would want to improve if they had the opportunity for it. As the respondents were provided with a free text field to answer, the responses varied considerably from very definite to very broad answers. A combination to NCWF main level categories was conducted to produce somewhat comparable results. According to the responses, most of the desired increases in expertise are of a technical nature. The most desired improvements in expertise were on penetration testing with 13 responses from a total of 44 responses, shown in Figure 13. As discussed in Chapter 5.1.9, networking and programming expertise were also among the most desired improvements of expertise. The results fit the current landscape, as technical platforms evolve and require ever more effort to stay on the edge of new technologies.

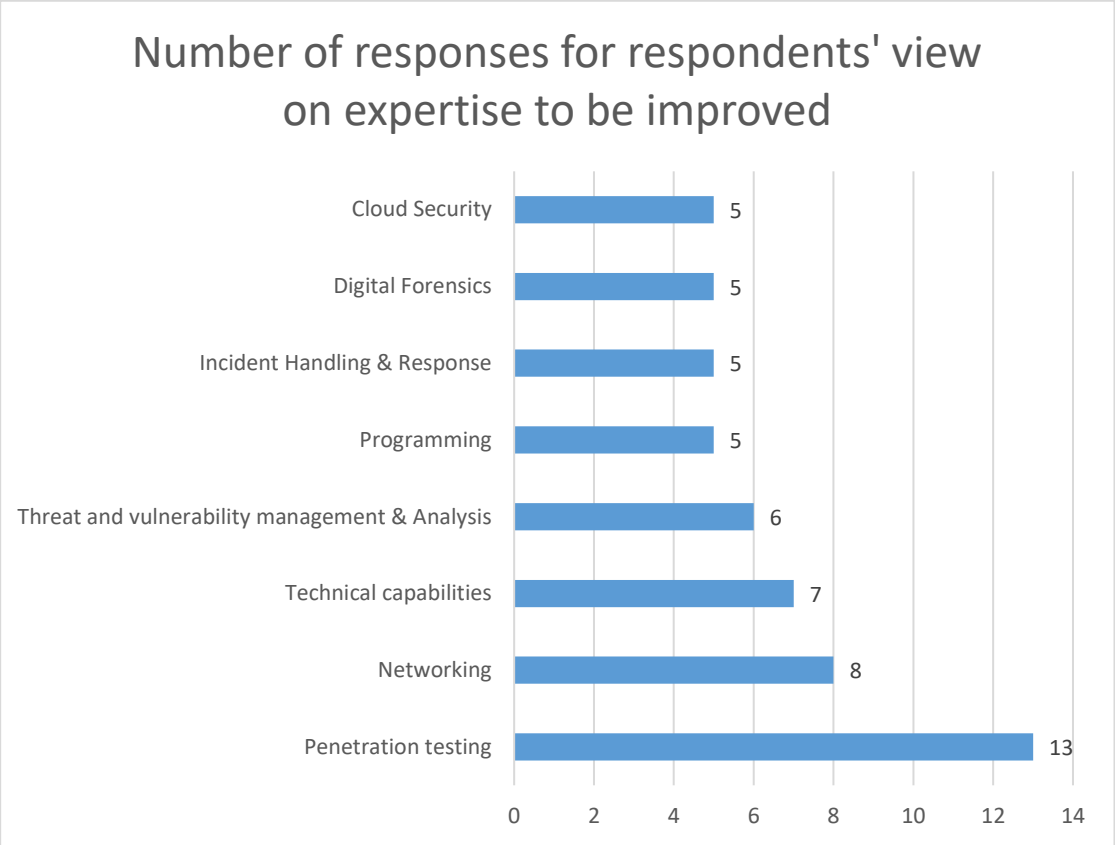


Figure 13: Respondents' view on most important areas of expertise to be improved

5.1.10 Expertise requiring more attention at the start of a career in cyber security

Respondents were asked whether some expertise should have received more attention or training at start of their career. Again, data was combined to obtain a higher-level overview of subject areas. As only three categories had five or more responses, five categories with the most responses were included in the analysis. The most common skill to be improved at the start of the career was programming as shown in Figure 14. Networking and technical capabilities were found among the top five responses as in previous questions. Additionally soft skills and business management were included in the most common responses, even though these areas are not directly related to cyber security.

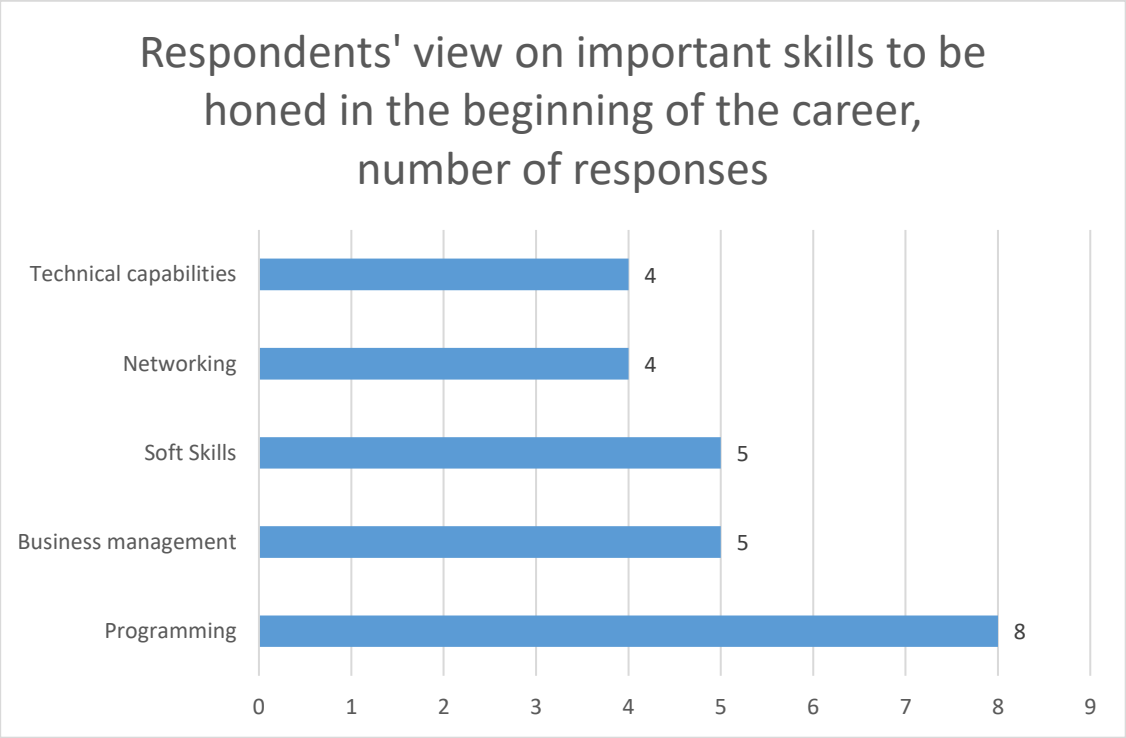


Figure 14: Respondents' views on common skills requiring more attention at the beginning of the career

5.1.11 Recruiters' views on weak areas of expertise in recruits

Respondents working in a recruiter position were asked which area of expertise was most commonly missing from the recruits. Answers were combined to NCWF main level categories to provide a higher-level overview of the responses. As shown in Figure 15, from 31 responses, soft skills were the weakest area with eight answers, followed by technical capabilities with seven answers, networking with five and programming with four answers. Threat modeling emerged as a new top five area of expertise with three answers.

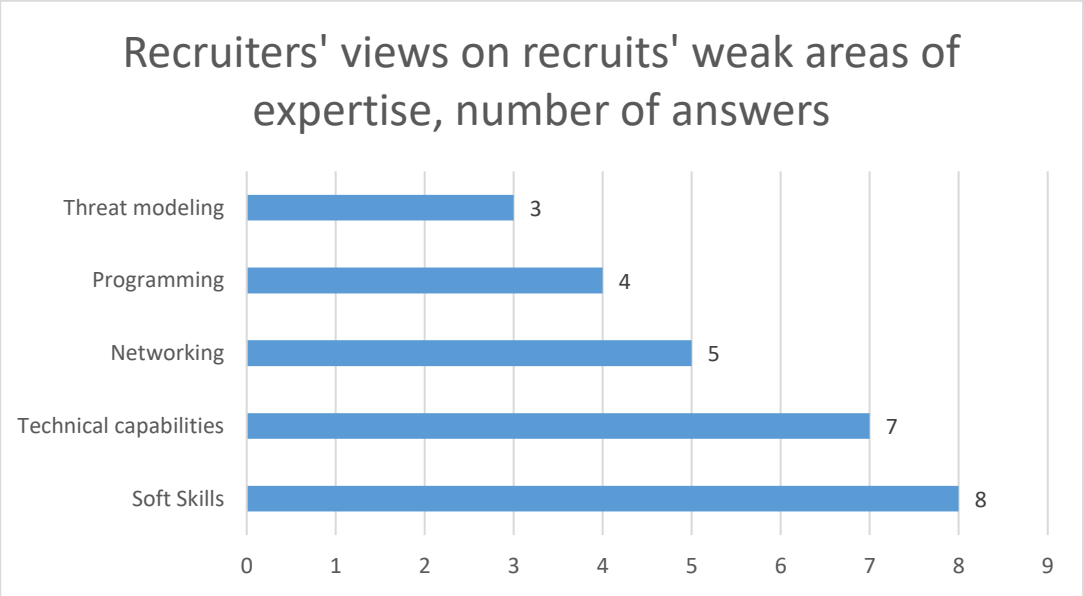


Figure 15: Recruiters' views on skills often missing among the recruits

5.1.12 Other suggestions to improve cyber security education

In the final question, respondents were asked for suggestions on how to improve cyber security education. Similarly to previous cases, the answers were categorized into NCWF main level categories for a broader overview of the results. As the number of responses was over five for only one main subject, the response data of five responses with most answers were used. As the fifth and sixth most common categories had same amount of answers from the total of thirty responses, the sixth category was included in the analysis as well.

The Specialization category consists of answers which felt that cyber security education should be more specialized within a specific subfield inside cyber security, for example, a degree programme specializing into digital forensics.

The Deep knowledge of technology category contains answers suggesting focusing on specific technology and education of higher-level expertise.

The Business management and relation to business category contains responses which suggested including a deeper business aspect to the education, and training on how cyber security supports the business.

Soft skills include responses that suggested including courses and teaching focused on different soft skills, such as teamwork, systems thinking and other related soft skill areas. As a research note, soft skills are already included partially in different curriculums in form of technical writing and team projects. However, these do not fulfil all aspects of soft skills.

The Lifelong learning, current technology and trends category included answers suggesting teaching students that the cyber security field requires constant development and learning, as technology renews without a pause. One answer suggested developing the curriculums in tandem with current and future threat intelligence, in order to better prepare the students for a contemporary cyber security environment.

Core technical skills gained the most answers as shown in Figure 16. According to respondents, it is not uncommon that graduating cyber security students are missing the basic core skills in ICT required in a cyber security job. As an example, a suggestion was made to layer cyber security degrees on top of a networking or a programming degree. The suggestion seems to be valid, as the same areas of expertise emerge in every set of answers.

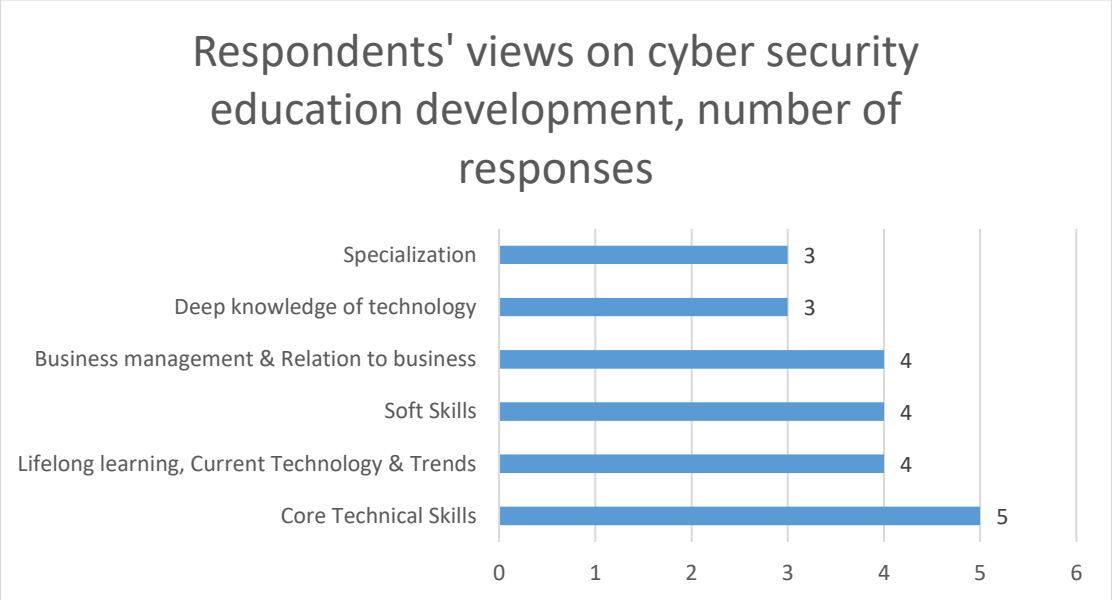


Figure 16: Respondents' view on how universities could develop their cyber security education

5.2 Comparison of curriculum and questionnaire data

This chapter focuses on comparing the collected curriculum data with questionnaire respondents' answers. The collected curriculum data contained a total of 2089 rows of course data across graduate and undergraduate level degrees in the United States and European Union. Graduate level education included 501 courses in the United States and 536 courses in European Union. Undergraduate level education included 546 courses in the United States and 506 courses in European Union.

The curriculum contents are compared to answers obtained from questionnaire sets, to each question in turn, starting with the answer obtaining the most responses. The comparison is limited to the number of categories analyzed within a single question's answer set, as described in subsections under Chapter 5.1. The comparison results are expressed as three separate figures. The figures depict the course names, course types (mandatory, elective, etc.) and number of different programmes offering the course. Further analysis is performed on the most common NCWF categories in course data. Some responses are categorized in more than one NCWF category but only the first mentioned category is used in the analysis. More detailed information, such as used search words to obtain the course information for NCWF categories for data comparisons, are attached in Appendices 10-12.

5.2.1 Comparing course data to most important areas of expertise identified by questionnaire respondents

Chapter 5.1.9 examined the most important areas of expertise identified by questionnaire respondents. This chapter focuses on comparing the most important areas of expertise to the collected curriculum data in more detail.

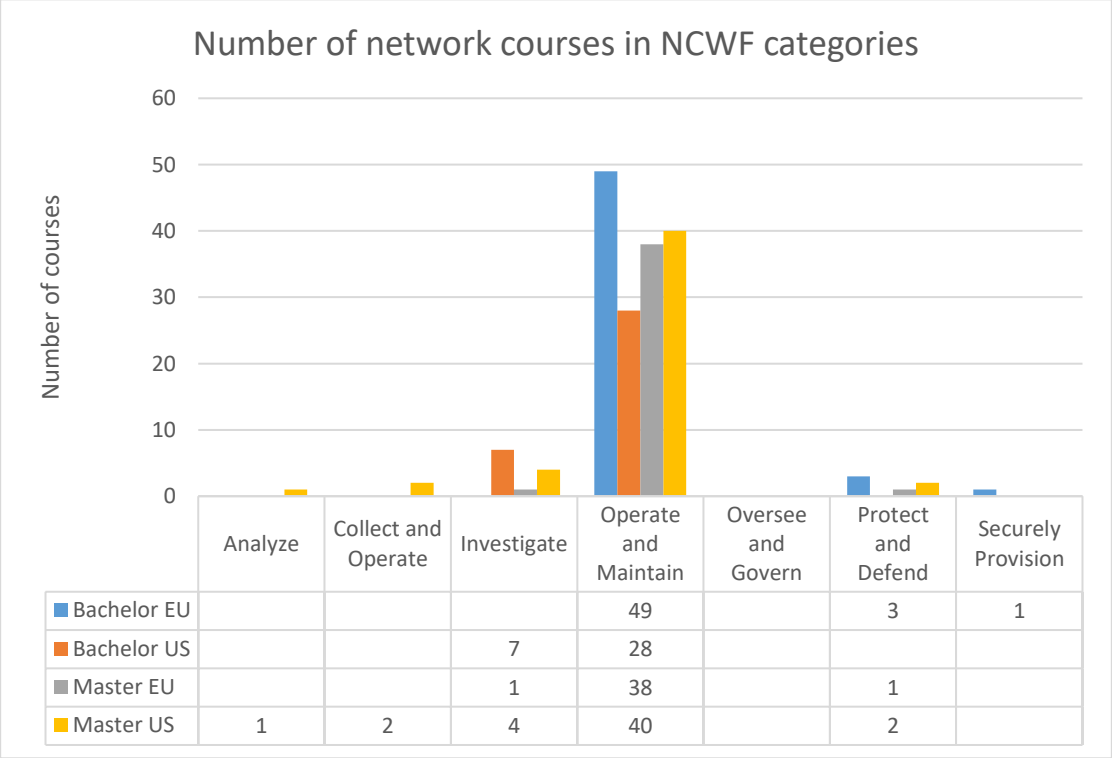
Soft skills

Soft skills are personality and behavioral attributes, such as decision making, communication abilities, teamwork, and adaptability. Some soft skills can be trained, such as teamwork, however most of the soft skills cannot be taught. Soft Skills play an important part when forming teams in work, and currently many recruiters rank soft skills higher than technical skills, as technical skills are easier to teach. (Soft Skills, 2020.)

As soft skills are too broad to be categorized according to NCWF categories, course comparison cannot be effectively performed in the same manner as with other skills. It is, however, noteworthy to mention that soft skills were considered the most important area of expertise by the questionnaire respondents, and special attention should be paid by the universities in ensuring that students are taught a wide variety of soft skills to the extent possible in a degree program.

Networking

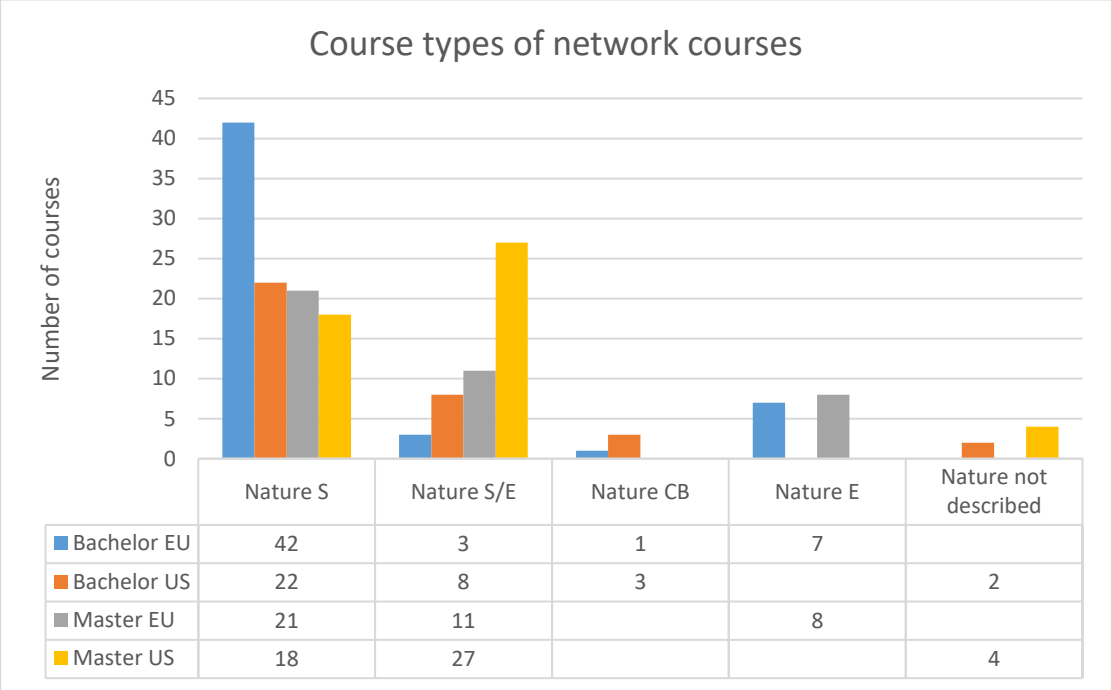
The category split between NCWF categories and count of course offerings for all education levels in scope are expressed in Figure 17. The majority of the courses fit the "Operate and maintain" category of the NCWF framework, with the "Investigate" category being the second most common category. Networking courses were mostly categorized into the "Operate and Maintain" category as the courses focused on core network skills, while the "investigate" category consists mainly of network forensics courses.



	Analyze	Collect and Operate	Investigate	Operate and Maintain	Oversee and Govern	Protect and Defend	Securely Provision
Bachelor EU				49		3	1
Bachelor US			7	28			
Master EU			1	38		1	
Master US	1	2	4	40		2	

Figure 17. Number of network courses in degrees across NCWF categories

A combined total of 107 mandatory network courses and a total of 64 elective or specialization/elective courses were available for students, as shown in Figure 18. Most of the network courses are of specialization type, followed by specialization/elective, meaning that the course is a part of modular curriculum.



	Nature S	Nature S/E	Nature CB	Nature E	Nature not described
Bachelor EU	42	3	1	7	
Bachelor US	22	8	3		2
Master EU	21	11		8	
Master US	18	27			4

Figure 18. Number of network courses for each course type

Analysis of the course data shows that 61 out of 69 degree programmes offer networking courses in some form. The distribution of these courses across degree levels and locations is shown in Figure 19. A possible reason for why multiple universities did not offer any networking courses could be that network studies are embedded within another course. For example, Saarland University's Bachelor of Science in Cyber Security did not include any pure network courses but had some network topics embedded to their "Basics of Cyber Security" course.

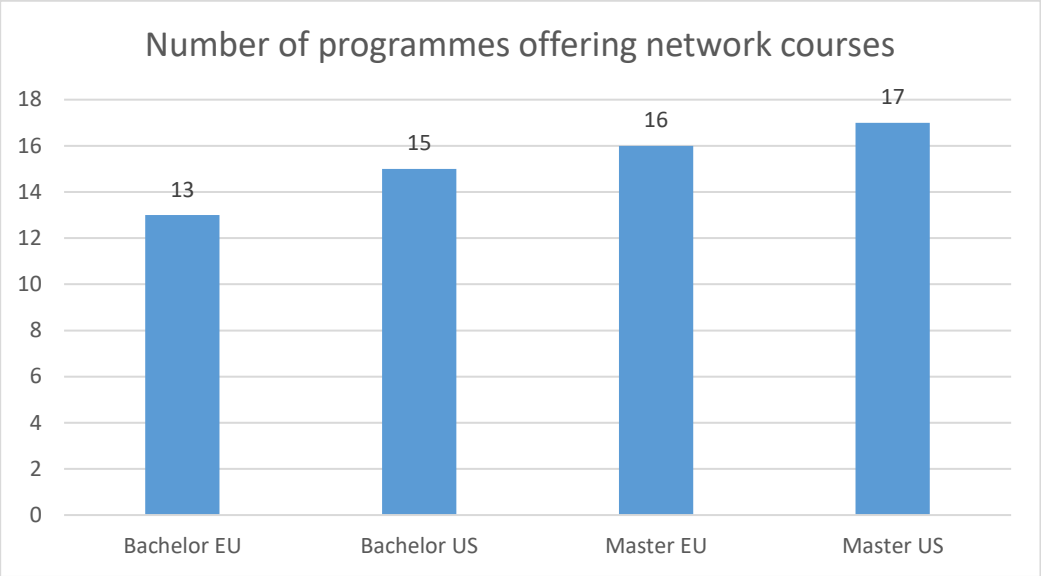


Figure 19. Number of degree programmes offering network courses

Risk Management

The second most highly ranked area of expertise in the questionnaire was Risk Management. Risk management NCWF categorization includes two main categories: Securely Provision and Oversee and Govern. Due to the nature of the categories of the courses, most of the courses fall under Securely Provision category, shown in Figure 20. As an example, Risk Management courses were categorized as Securely Provision within the NCWF, while Cyber Risk Strategy and Governance courses were included in Oversee and Govern category, as Cyber Risk Strategy is limited to cyber domain risks, whereas Risk Management overlaps with other business area risks as well.

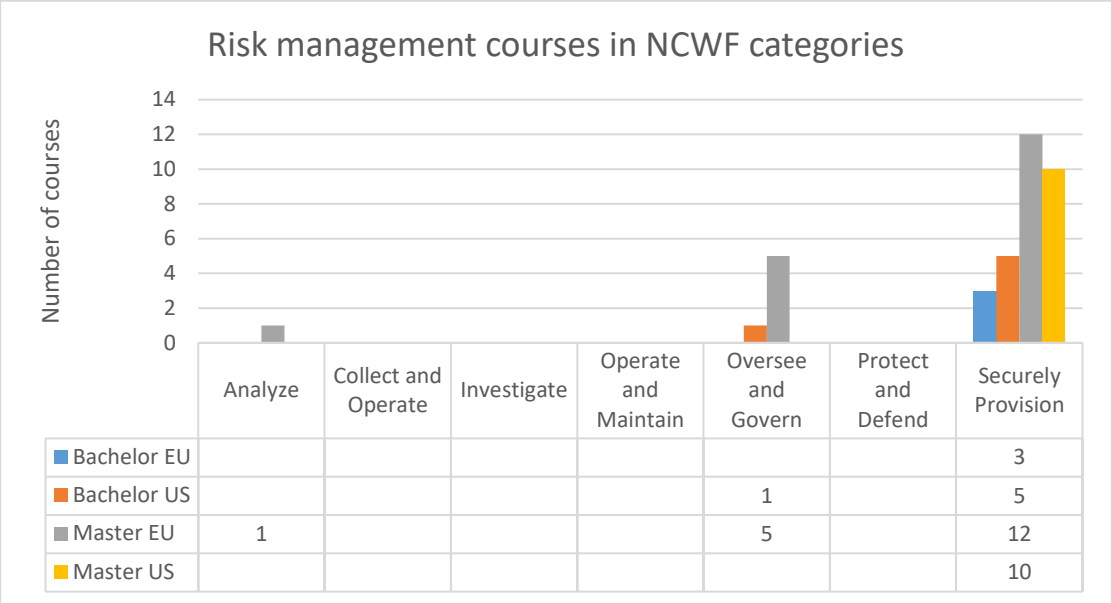


Figure 20. Number of Risk Management courses in NCWF categories

As with networking courses, most of the risk management courses are specialization courses or specialization/elective by their nature. However, compared to networking courses, a higher percentage of courses were elective, as shown in Figure 21. Graduate degrees in the European Union included more mandatory Networking courses than any of the other counterparts, with a total of 14 Networking courses across the degrees.

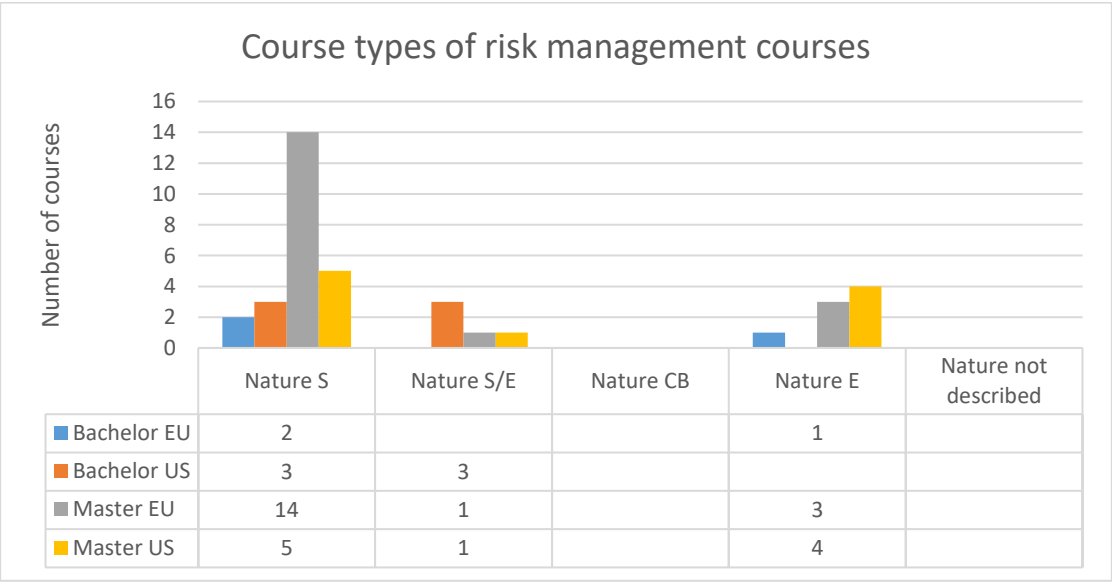


Figure 21. Risk Management Course Nature distribution

The collected data consists of a total number of 37 courses on risk management across 26 universities. As seen in Figure 22, graduate level degrees offer more Risk Management courses than undergraduate level courses, perhaps as a result of the expectation that graduate level graduates will end up in more managemental roles, for which studies in Risk Management are useful. At the undergraduate level, European Union based degrees offer less Risk Management courses than their United States counterparts. Overall, the availability for risk management courses is drastically lower when compared to Networking courses, even though the area of expertise is ranked high in the most important areas of expertise by stakeholders.

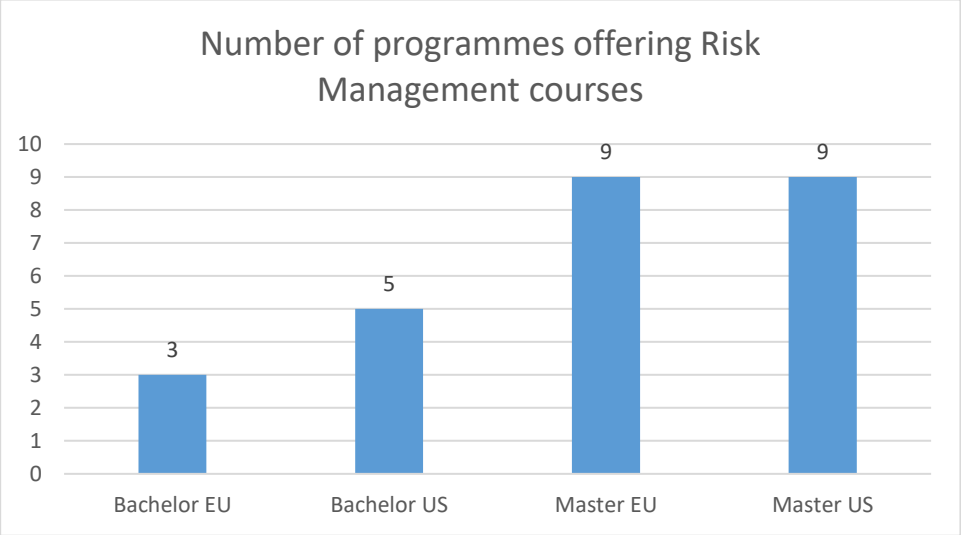
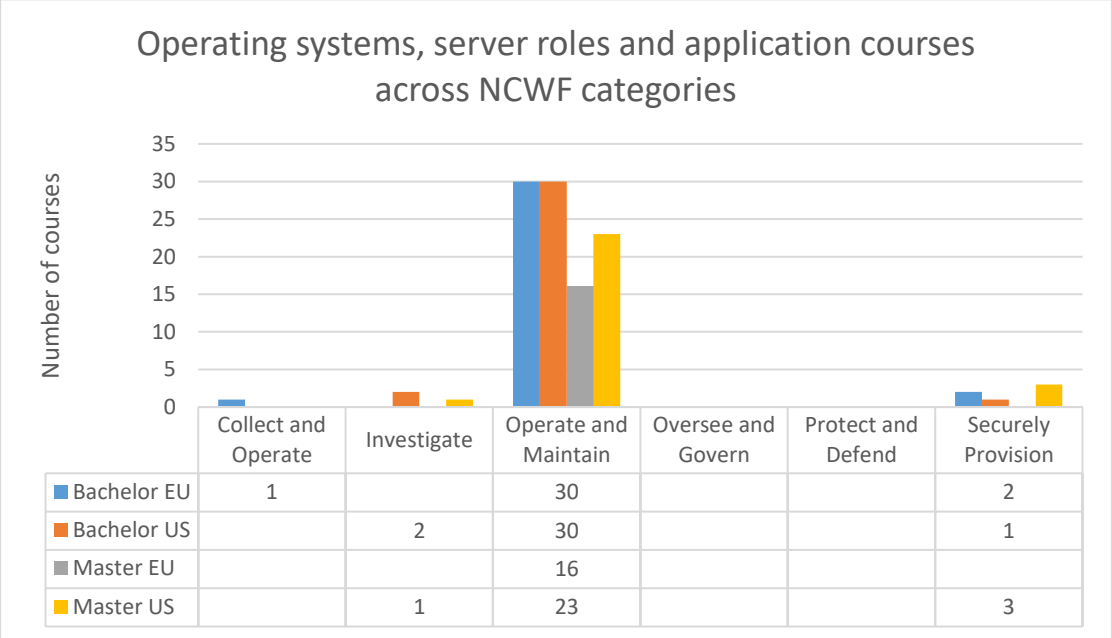


Figure 22. Programmes offering Risk Management courses

Operating Systems, Server Roles and Applications

Operating Systems, Server Roles and Applications ranked third among the aspects considered to be most important by questionnaire respondents. This was not unexpected, as a major part of cyber security is understanding the environment and configuring the platforms correctly. Most of the relevant courses fall under Operate and Maintain category of NCWF, while a small amount of courses land under the Securely Provision, Investigate and Collect and Operate categories, shown in Figure 23. Distribution of courses across multiple categories is a result of the contents of the course

and the data analysis method used to categorize courses. As the curriculum data is analyzed with searches using key words such as “Windows”, the course “Windows Forensics” would land at the Investigate category NCWF, as this category holds the forensics related expertise. A “Windows Servers” course, on the other hand, would better fit the Operate and Maintain category, as the course focuses on the basic administrative and operational side of Windows server infrastructure, instead of taking a forensic aspect.



	Collect and Operate	Investigate	Operate and Maintain	Oversee and Govern	Protect and Defend	Securely Provision
Bachelor EU	1		30			2
Bachelor US		2	30			1
Master EU			16			
Master US		1	23			3

Figure 23. NCWF category distribution for Operating Systems, Server Roles and Applications courses

The collected course data suggests that the course type distribution differs between courses in the United States and the European Union based degrees, especially at graduate level. In the European Union, courses focused on Operating Systems, Server Roles and Applications are often mandatory, shown in Figure 24. In the United States, courses falling under this category are often elective, especially at graduate level degrees.

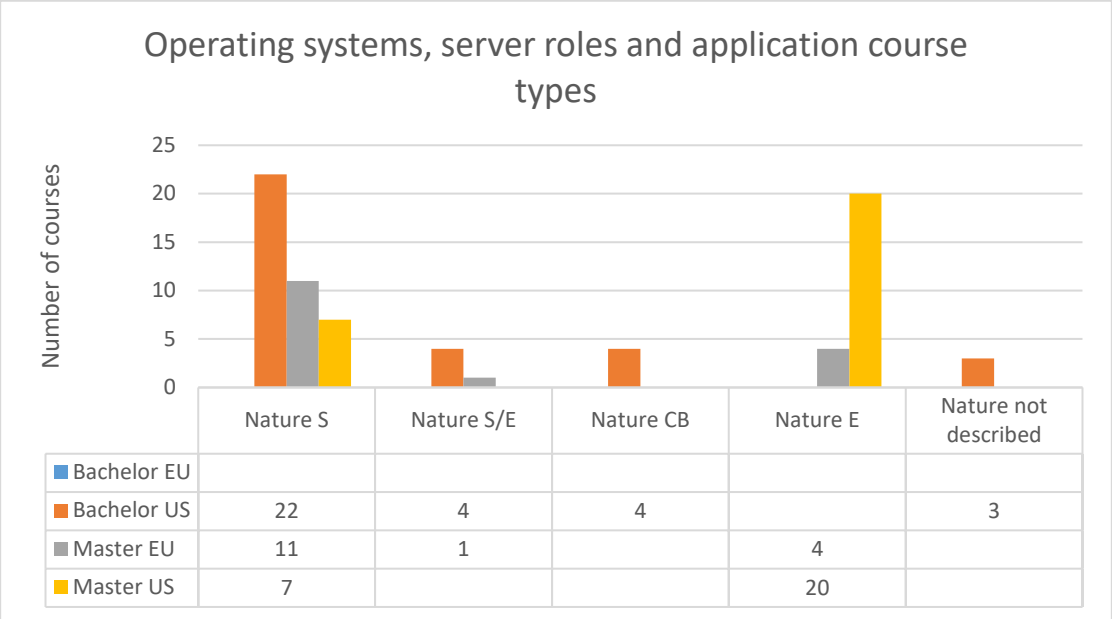


Figure 24. Number of Operating Systems, Server Roles and Applications courses in each course type category

Undergraduate level degree programmes offer more courses in the category compared to graduate level, as shown in Figure 25 below. A possible explanation is that some graduate level programmes offer more management-oriented education, which often keeps the number technical courses relatively low.

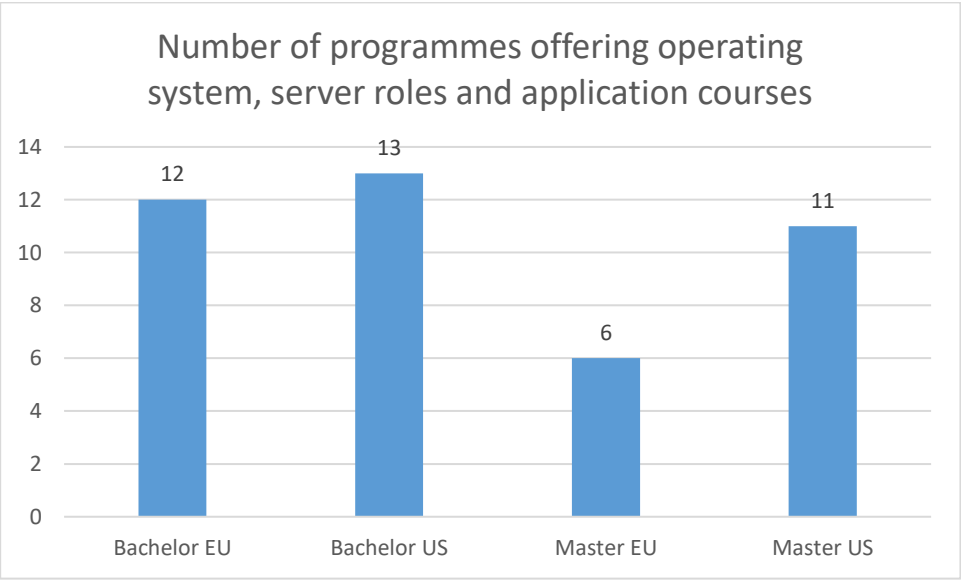


Figure 25. Number of degrees offering Operating Systems, Server Roles and Applications courses

Programming

NCWF category distribution for programming courses was unambiguous with nearly all courses falling under “Securely Provision” NCWF category, as seen in Figure 26. Only one course was included in “Investigate” category – this specific course was a graduate level course “Programming for Digital Forensics” provided by Lewis University in the United States, with the content of the course more oriented towards the Investigate category of NCWF.

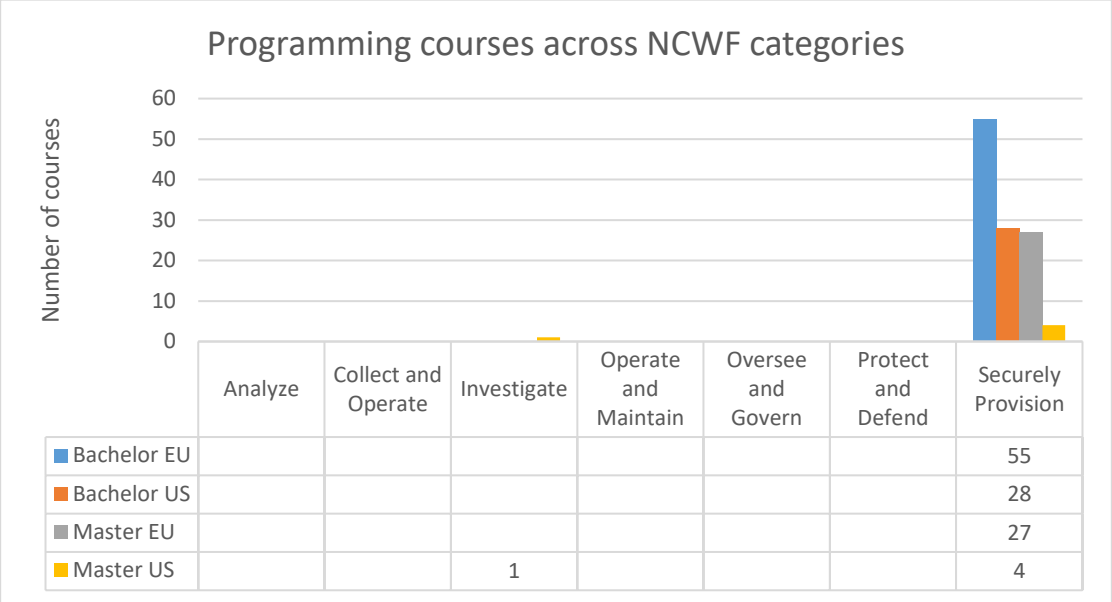


Figure 26. Number of programming courses in each NCWF category

Programming studies are more readily available at the undergraduate level than at graduate level – Figure 27 shows that European Union based universities provide more programming studies in both mandatory and elective studies when compared to the United States. It is also worth mentioning that there are no completely elective programming courses available at the United States undergraduate level, indicating that programming skills cannot be improved beyond the scope of the mandatory sections of the degree.

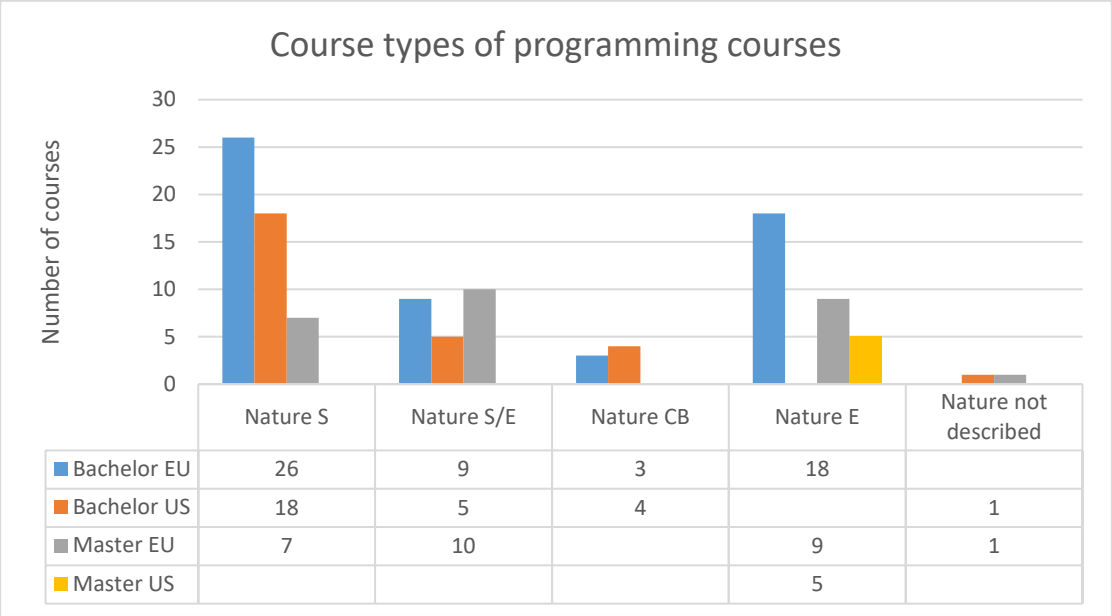


Figure 27. Number of programming courses available across course types

41 out of 69 degree programmes offer programming courses. At the undergraduate level, 27 degree programmes – 90% of the programmes – offer at least one course of programming. At the graduate level, this percentage drops to 35%, with only 14 degree programmes out of the 40 programmes included in the research data offering programming courses. The total number of programming courses is considerably higher at the undergraduate level compared to the graduate level, as seen in Figure 28.

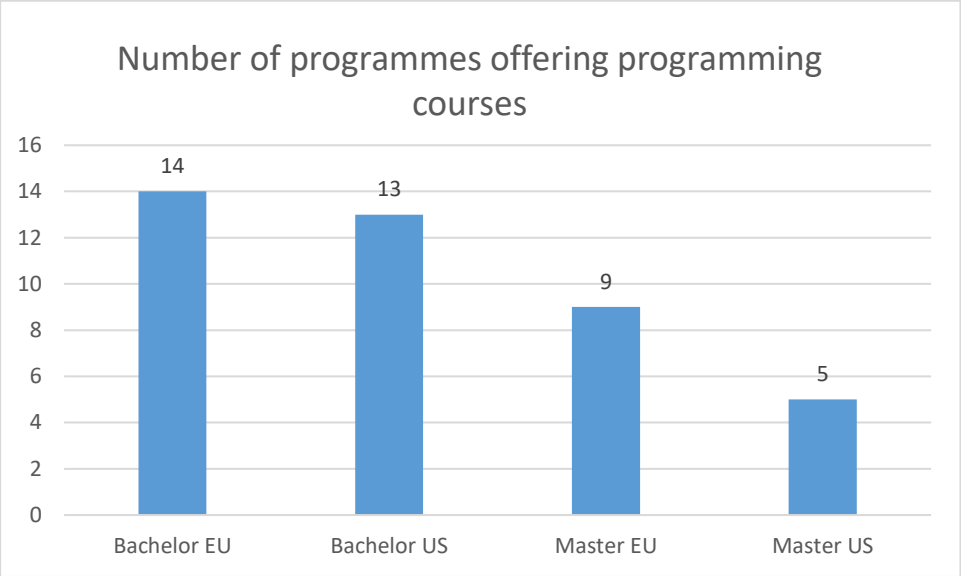


Figure 28. Number of degree programmes offering programming courses

Incident Response

Incident Response and topics related to Incident Response received the fifth most answers to the question of important areas of expertise. Across the collected course data, Incident Response had a total course count of 15. The NCWF classification for these courses is split between the Protect and Defend category and the Investigate category, with most of the courses focusing on the Protect and Defend side of the classification, as seen in Figure 29. Courses were attributed to the NCWF Investigate category when the courses included aspects of forensic investigations in incident response.

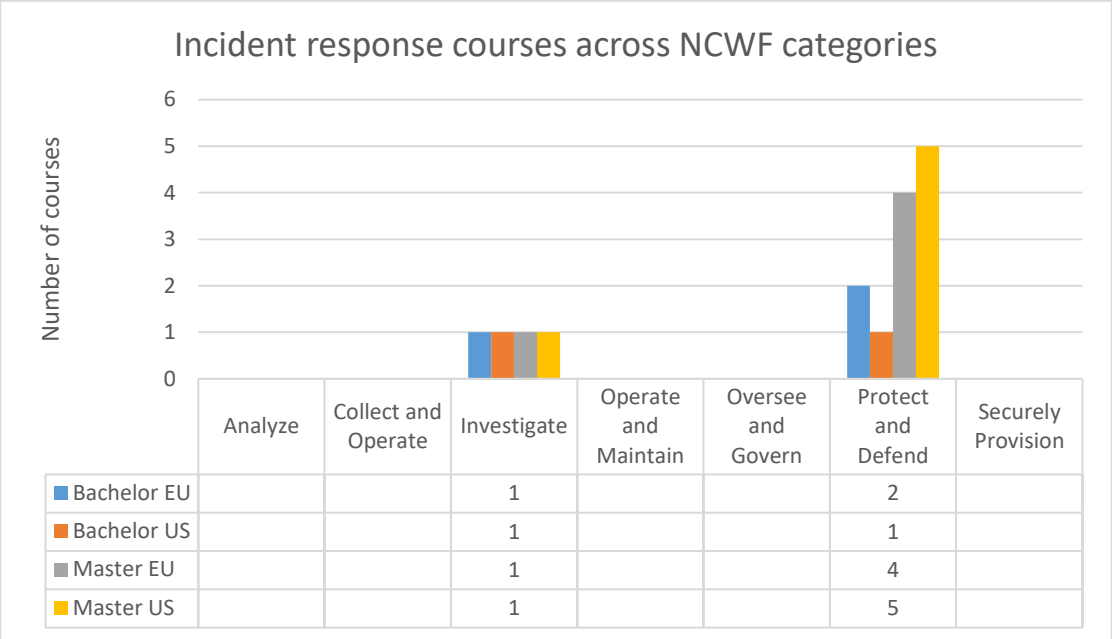


Figure 29. Number of Incident Response courses across NCWF categories

Of the total number of Incident Response courses, 60% were mandatory and 40% elective courses. The specific distribution shown in Figure 30 shows that the United States undegraduate level degrees only contained mandatory Incident Response courses, with no elective courses available. The elective nature of course can mean two things – either students outside of cyber security programme can attend the course, increasing security awareness and incident management abilities more widely, or cyber security students could choose something else as an elective and miss expertise classified as important among the stakeholders.

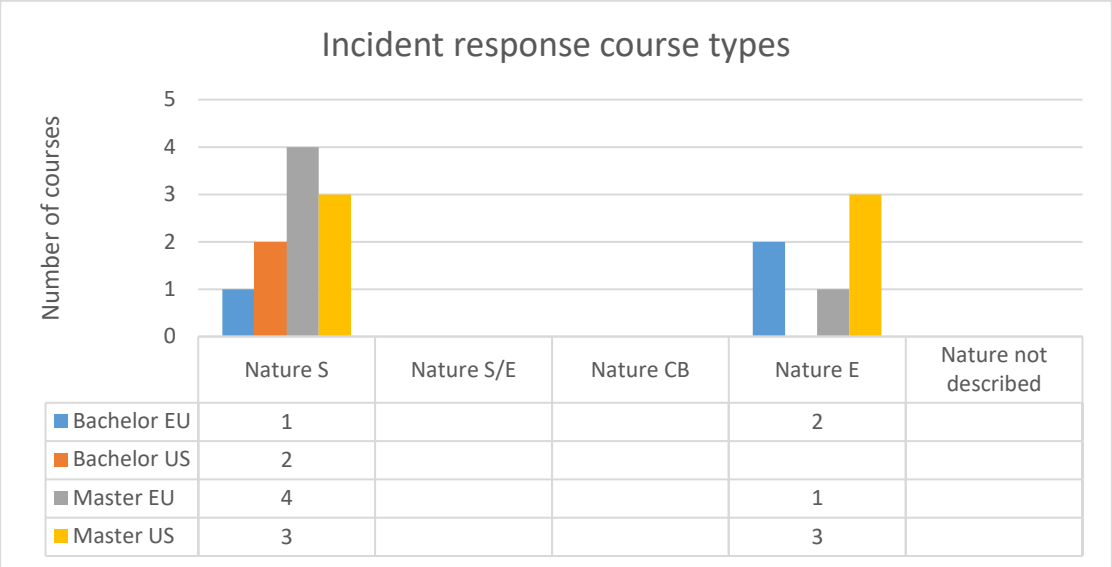


Figure 30. Number of Incident Response courses across course types

Only a total of 13 degree programmes, accounting for 18% of all degree programmes, offer Incident Response courses. Figure 30 shows the fairly even distribution of these courses across different locations and study levels, however, trends are difficult to detect as the offering of Incident Response courses is at such a low level. Of the over 2000 courses analyzed, only 15 courses were Incident Response courses. Even Incident Response expertise was partially covered in generalized cyber security courses, the availability of courses was noticeably low. Compared to stakeholder demands covered previously, Incident Response is the first area of expertise which has a noticeable gap between the course offering and the perceived importance.

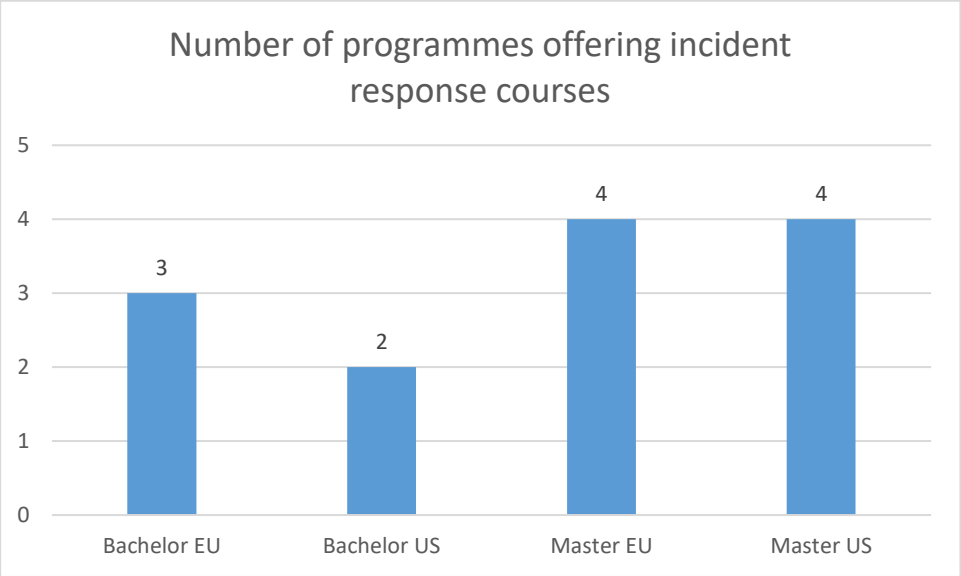


Figure 31. Number of degrees offering Incident Response courses

Education and Training

Education and Training as an area of expertise might sound vague or unrelated, considering that students are learning to become professionals in cyber security. However, educating end users and increasing security awareness is important task among the stakeholders, and not always the easiest task as workforce in enterprise-level companies come from different backgrounds. For example, one user could easily detect different threats related to cyber security, whereas another user might input their credentials to every portal and e-mail requesting them. Both users still need cyber security training and awareness tailored to fit their work in order to reduce risks towards the company, and the design and implementation of this training often falls to the cyber security professional. Figure 32 shows that only a total of two courses of Education and Training were available across all degrees – one at graduate level in the United States, one at undergraduate level in European Union, both of which were categorized into Oversee and Govern category of NCWF.

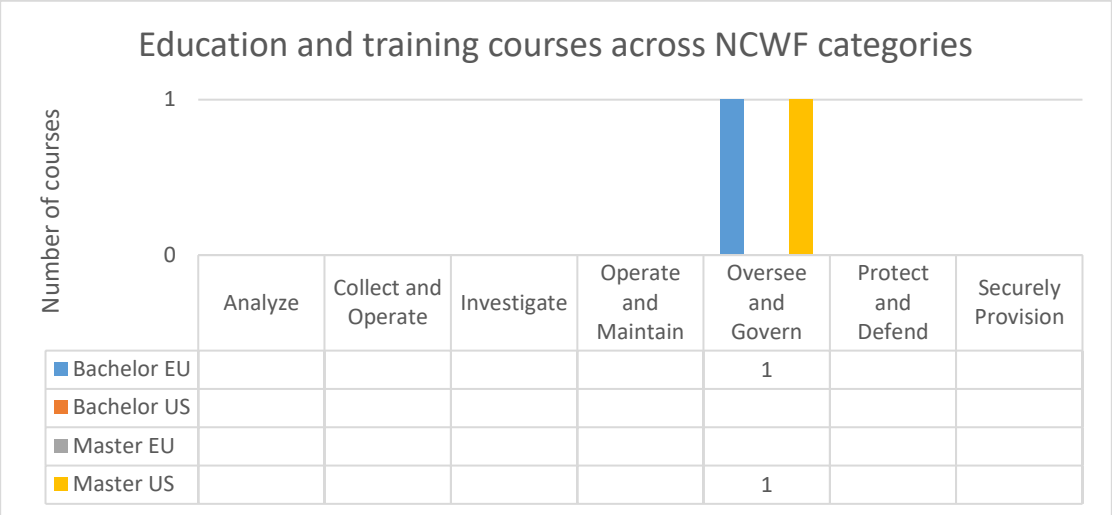


Figure 32. NCWF categorization and available courses for Education and training

The percentage is alarmingly low when considering a statement by Kaikko (2016), indicating that phishing against end users is a highly effective method to gain a malicious foothold in organizations. The situation is even more dire, as one of the only two courses available is elective, as seen in Figure 32.

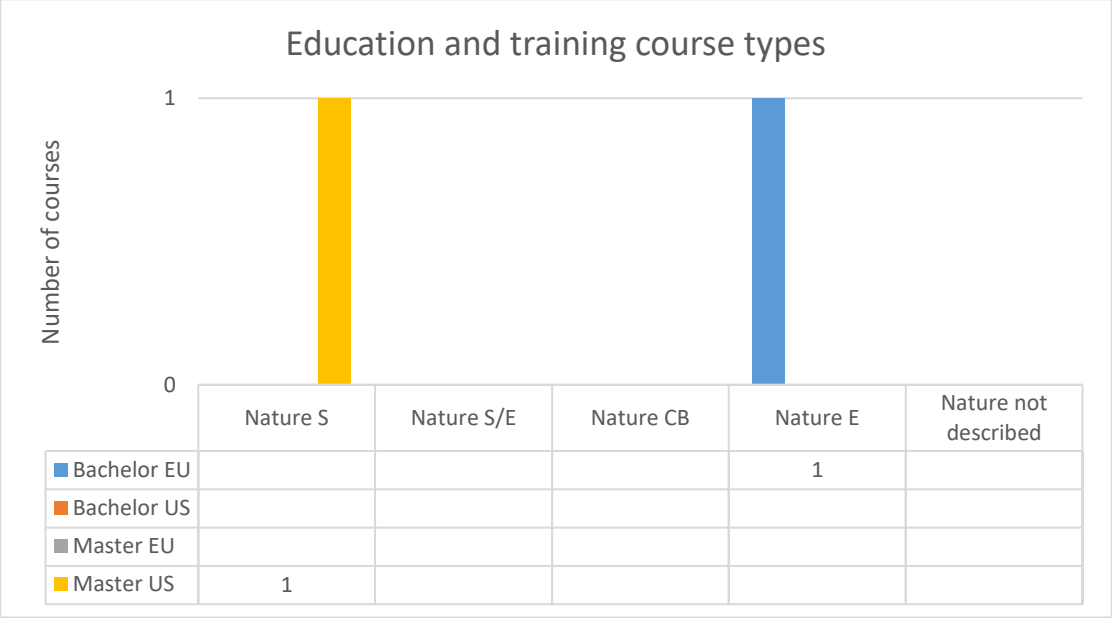


Figure 33. Number of Education and Training courses in each course type

The programmes offering the courses are a single undergraduate programme in European Union, and a single programme at graduate level in the United States, shown

in Figure 34. Even though the area of expertise may be partially covered in other courses, the area of expertise could receive more attention in the form of courses targeted at teaching and educating end users.

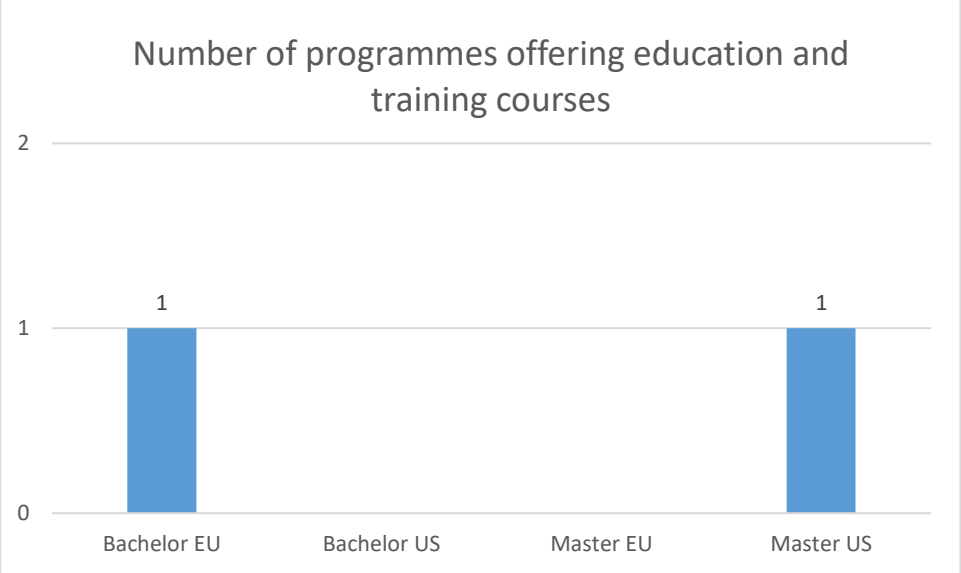


Figure 34. Number of programmes offering Education and Training courses

Penetration Testing

Penetration Testing courses included courses aimed at offensively evaluating target software and environments. Red Teaming was also included in Penetration Testing category courses, as even though the specifics and processes are different, the goal in both cases is the same: to penetrate the premises of an organization. Figure 35 shows most of the courses falling under “Protect and Defend” category of NCWF.

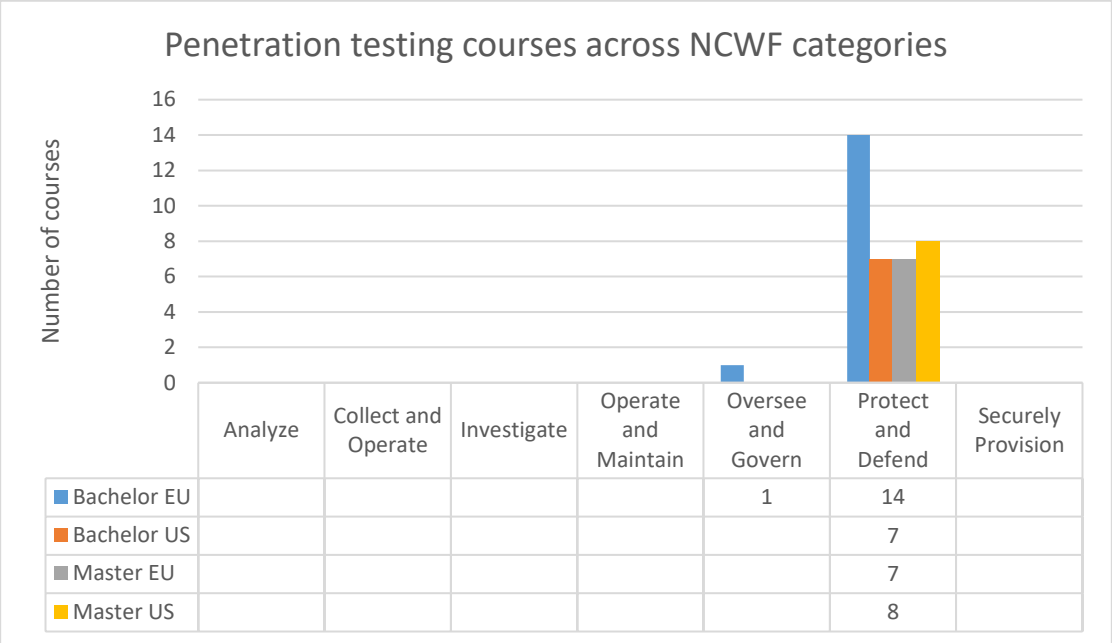


Figure 35. Number of Penetration Testing courses across NCWF categories

Majority of courses are mandatory specialization courses, except in graduate level in the United States, where the majority courses are available as elective, shown in Figure 36.

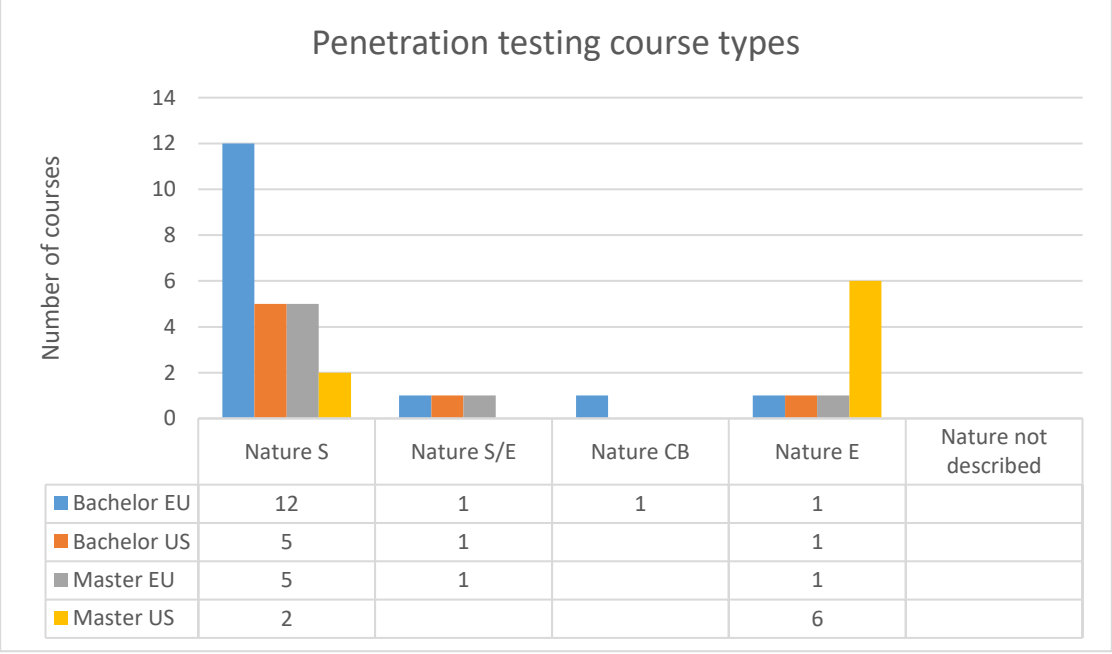


Figure 36. Number of Penetration Testing courses in each course type

Figure 37 shows that penetration testing courses are more prevalent in undergraduate level, even though courses are also available at graduate level. Undergraduate level degrees in European Union also offer more penetration testing focused courses than their United States counterparts. Penetration testing courses are only available in some degrees across all education levels and continents.

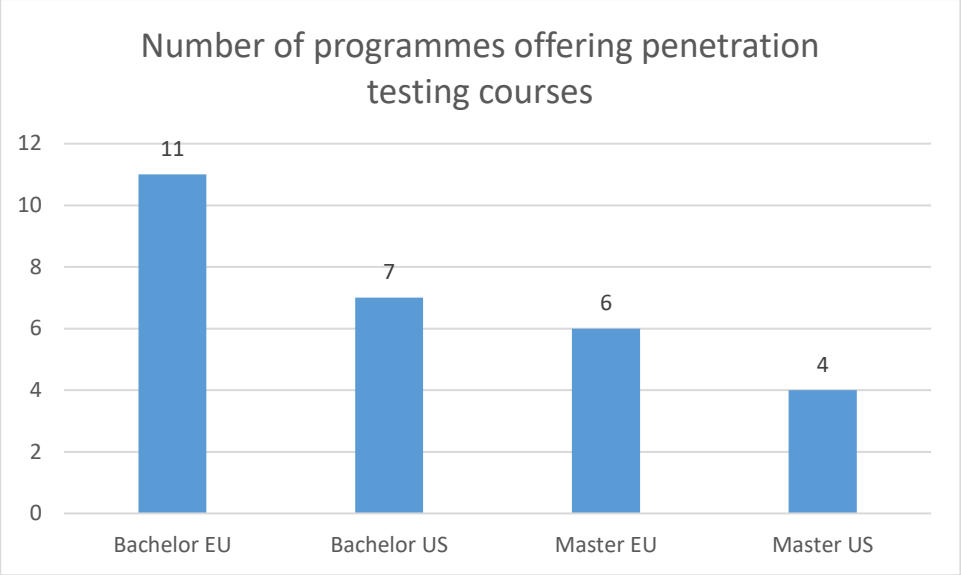


Figure 37. Number of Penetration Testing courses across degree programmes

Penetration Testing courses are commonly offered at undergraduate level, with European Union based universities having a slightly better availability for courses than their United States counterparts. This would indicate that the required training for Penetration Testing skills exists and the reason for the skill gap would need to be studied further.

Log and Security analysis

Log and Security analysis categorization includes areas of directly related expertise, such as a Security Analysis course, and a course that directly supports Security Analysis, such as big data analysis courses. The complete list of search words used to compile the list of courses is included as Appendix 9. Most of the courses fit the Analyze category of NCWF as the course focus is on log analysis and handling, shown in Fig-

ure 38, with a small portion of courses falling under Investigate, Operate and Maintain, Protect and Defend and Securely Provision categories of the NCWF. The courses falling under the secondary categories tend to approach Log and Security Analysis from a different perspective, warranting a different NCWF category.

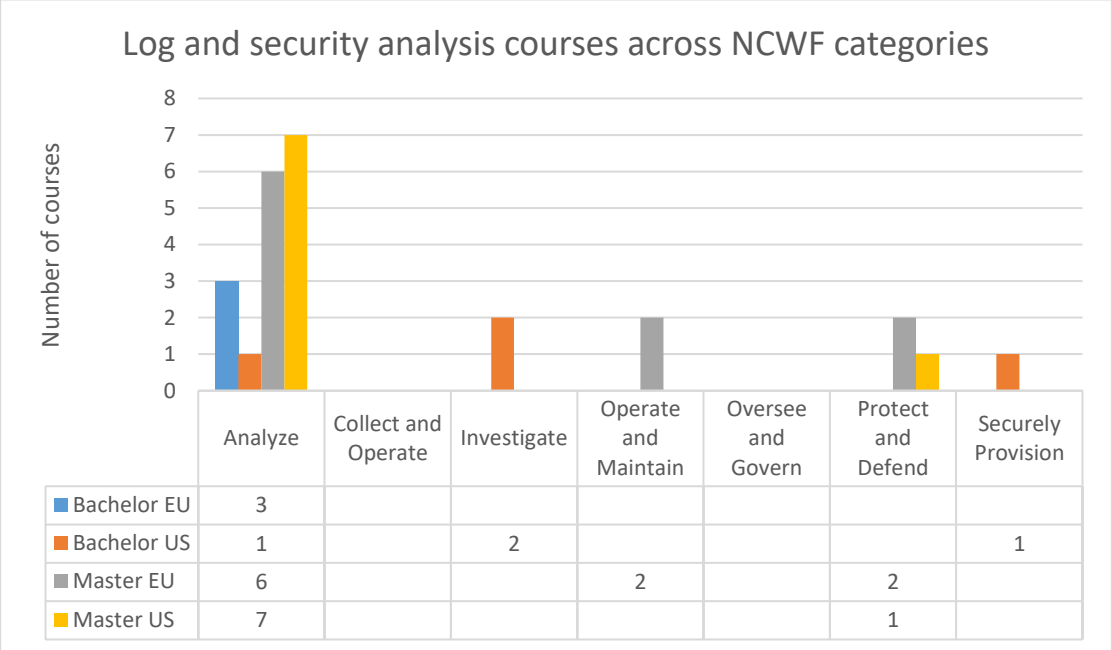


Figure 38. Number of Log and Security Analysis courses across NCWF categories

Course nature is distributed evenly between mandatory courses and elective courses when looking at the total number of courses. The United States undergraduate level degrees only included mandatory Log and Security Analysis courses, whereas graduate level degrees in the United States only included elective courses, shown in Figure 39. Only three Log and Security Analysis courses were available across all European Union undergraduate level degrees, whereas European Union graduate level degrees had a larger number of courses with a spread in terms of course nature. Course data analysis shows that the United States education system has focused the education of Log and Security Analysis at undergraduate level but offers elective courses at graduate level.

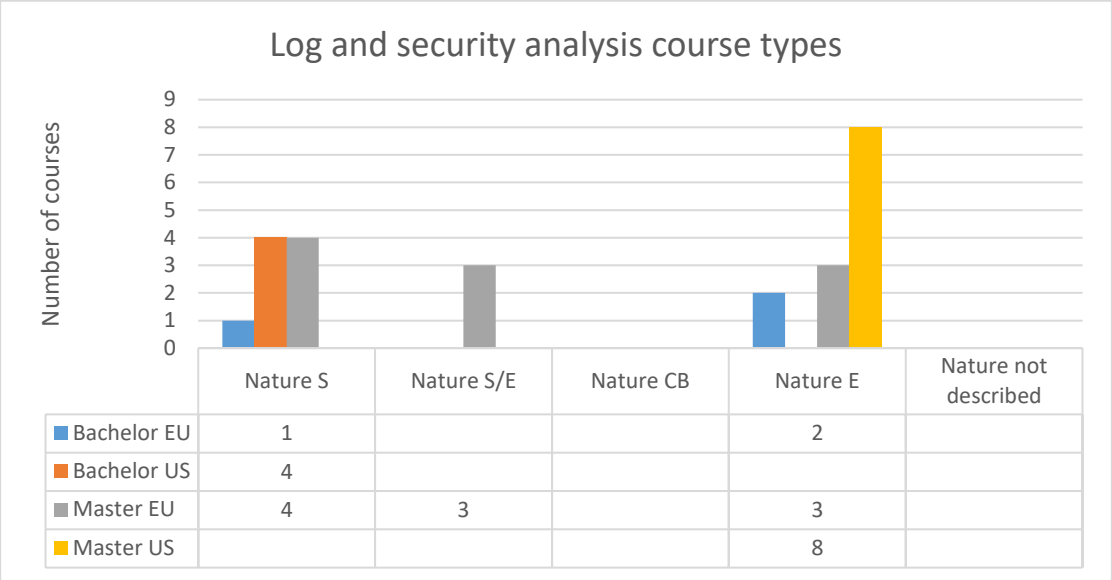


Figure 39. Number of Log and Security Analysis courses across course types

When comparing the programmes offering the courses and total count of courses across degree levels, the courses seem to be more targeted towards graduate level both in European Union and the United States, shown in Figure 40. However, as the United States based universities offer these courses as elective, the number of students enrolling in the courses remains unknown and determining whether the supply of Log and Security Analysis education meets the demand is impossible based on course title data alone.

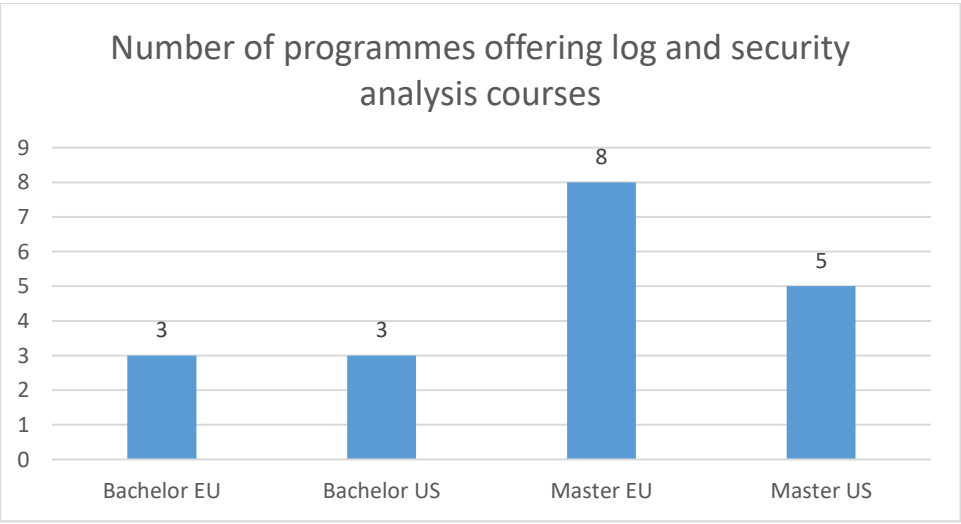


Figure 40. Number of degrees offering Log and Security Analysis courses

Log and Security Analysis is viewed as an important skill by stakeholders, however, analysis of course data shows that the offering focuses mostly on graduate level degrees and is lacking in terms of availability in most universities in European Union and the United States. The skill gap between recruit skills and stakeholder expectations is likely mostly caused by lack of courses available to students.

Forensics

Figure 41 shows that Forensics courses are more prevalent in the United States based universities when it comes to sheer number of available courses, with nearly all courses falling under the Investigate category of NCWF. Forensics as a concept also holds less variation in terms of course content compared to some of the other previously encountered courses, creating a more tightly focused NCWF Investigate category grouping.

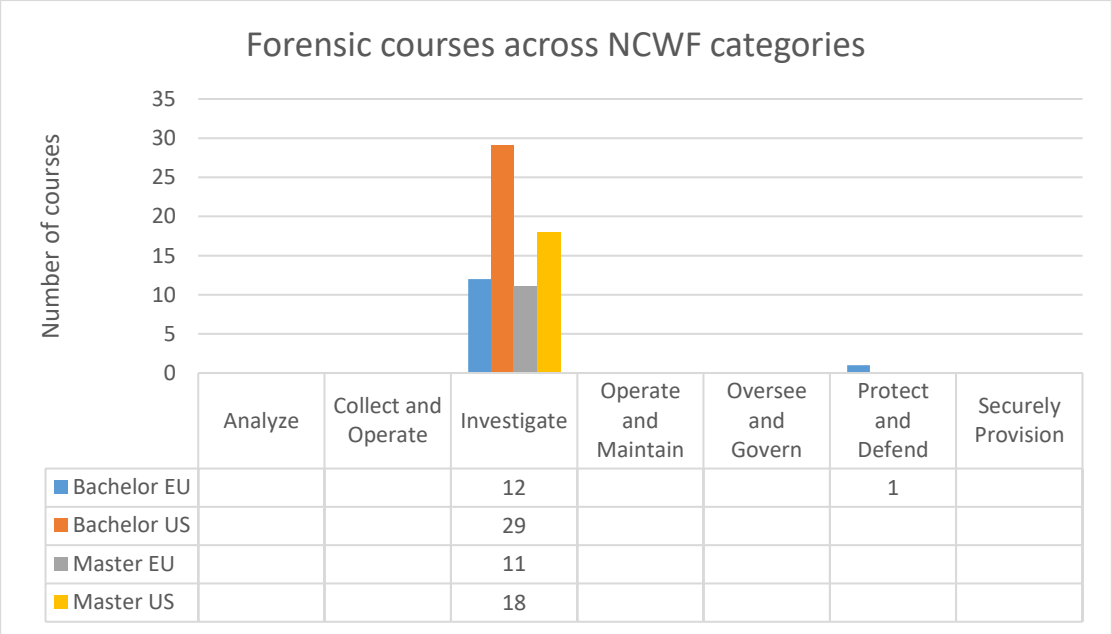


Figure 41. Number of Forensics courses across NCWF categories

The courses, however, have more variation in terms of course nature, shown in Figure 42. Elective nature is more common in courses especially in the United States based universities at graduate level than in European Union. As contrast, European

Union based universities only offer mandatory courses in Forensics with no elective Forensics courses offered. Otherwise the distribution of course natures lean towards mandatory courses.

	Nature S	Nature S/E	Nature CB	Nature E	Nature not described
Bachelor EU	12	1			
Bachelor US	19	4	1	2	3
Master EU	7	2		2	
Master US	3			15	

Figure 42. Number of Forensics courses across all course types

A total of 44 different degree programmes offer Forensics courses, accounting for most of the degree programmes, shown in Figure 43. Even though the total number of degrees offering Forensic studies is at a decent level, it should be noted that some degrees are specialized towards forensic studies, whereas some degrees had very minimal forensic education, indicating that the choice of university also significantly affects the amount of forensic education received.

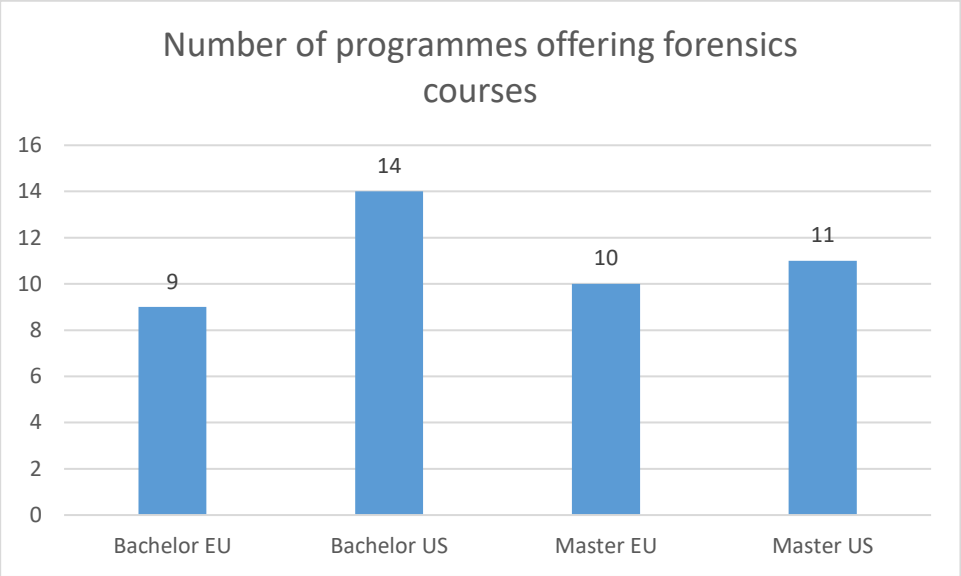


Figure 43. Number of programmes offering Forensics courses

Approximately half of the degrees available at both education levels and both examined regions contain some studies in Forensics. This would indicate that the availability of the courses is at a mediocre level, as not all students receive Forensics education, even when stakeholders consider this skill important.

5.2.2 Comparing course data to areas of expertise to be improved among the responders

Respondents were asked for three areas of expertise they would now improve if they had the opportunity. The response data was gathered to provide a view of expertise that existing cyber security workforce would study to further improve their expertise. This question attempts to show if some categories that are currently not included in curriculums are trending among the answers. However, the results from these comparisons should be viewed with caution, as the motivations behind skill improvement needs were not specified. Some of the perceived needs for skill improvement could indicate the need to refresh or update knowledge that has been previously studied, or simply showcase what respondents may consider fun or engaging areas of expertise to learn, rather than those specifically required for work.

Majority of the expertise areas to be improved are same as what the respondents considered the most important areas of expertise, however, two new areas of expertise also came up in the results: Cloud Security and Threat Analysis and Management.

Penetration testing

The area of expertise which received most of the responses with a significant margin was Penetration Testing. Penetration Testing offerings, distributions and categorization were analyzed in Penetration Testing subsection of Chapter 5.2.1. As Penetration testing was included in the most important areas of expertise and was clearly the number one of expertise improvement category, this would suggest that either the spread of courses or depth of the courses does not answer to the demands of the stakeholders.

Networking

Second most common answer in the response data was networking. Networking education availability and offerings within different degrees was outlined in Networking subsection of Chapter 5.2.1. As the majority of programmes include one or more Networking category courses, the need to improve Networking skills most likely is not a result of the availability of the courses, but rather the depth or contents of the courses.

Technical Capabilities

Technical capabilities were ranked as third in the category of expertise to be improved. This might very well be the result of operating systems, applications and tools receiving frequent upgrades and improvements, forcing the cyber security experts to update their knowledge to match the progress of new technologies. The improvement of technical capabilities is compared against course offerings for Operating Systems, Server Roles and Applications group, as the questionnaire response data mainly included answers categorized in this section of NCWF, such as operating systems and command line tools. Further analysis of course offering is available at Operating Systems, Server Roles and Applications subsection of Chapter 5.2.1. Course of-

fering analysis indicates that universities provide an ample set of courses for students, but the reason for the persisting mismatch between the skill gap and availability of studies is unclear and should be investigated further.

Threat Analysis and Management

Threat Analysis and Management was ranked as the fourth most common answer in the response data. Figure 44 shows that the NCWF category distribution of Threat Analysis and Management courses seems to be spread evenly, however, as the number of courses is small, no significant trends can be detected within course offerings. European Union undergraduate degrees had no courses focused on Threat Analysis and Management.

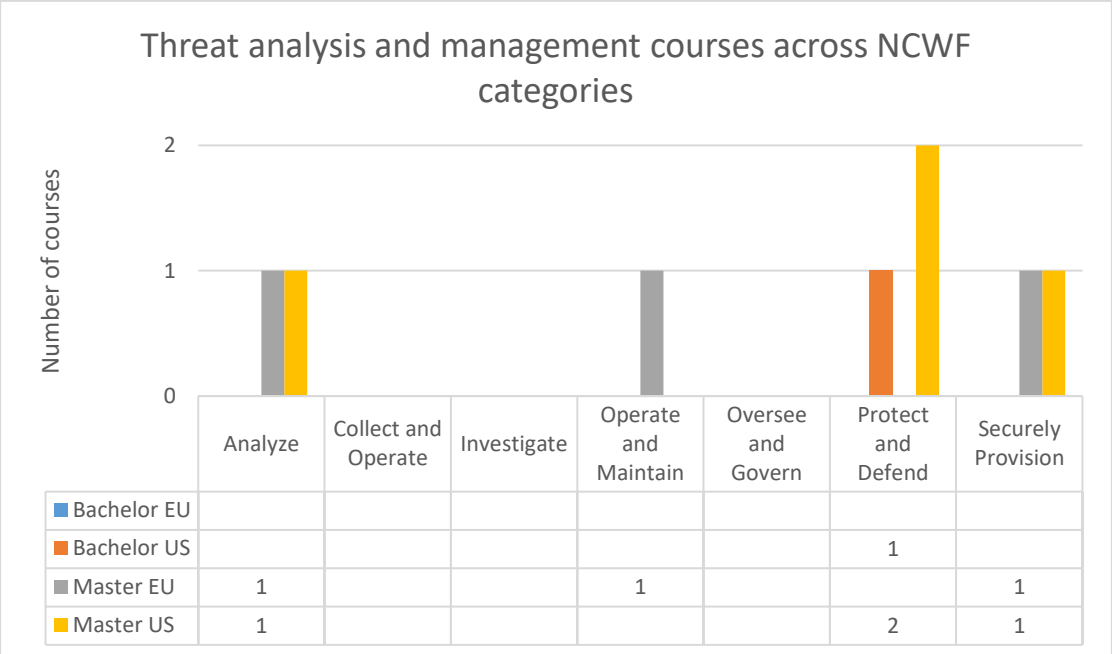


Figure 44. Number of Threat Analysis and Management courses across NCWF categories

The mandatory courses are included in undergraduate level studies in the United States and graduate level studies in European Union, as seen in Figure 45. Graduate level studies in the United States also offer mandatory courses if the student chooses the module including Threat Analysis and Management courses. Course offering

leans towards graduate level degrees, as only one course is available in a United States based university at undergraduate level.

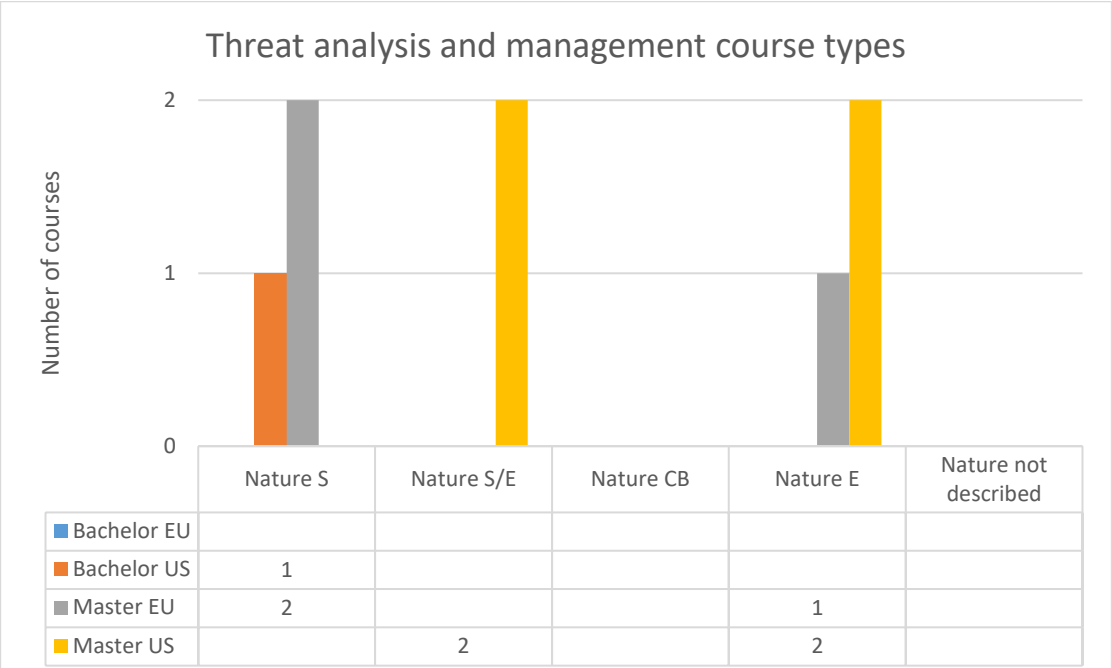


Figure 45. Course Nature distribution in Threat Analysis & Management

The low number of available courses indicates that either the area of expertise is not valued when designing curriculums, the depth of the subject is not enough for a focused course, or the area of expertise is embedded in overlapping courses, such as risk management or vulnerability management. Shown in Figure 46, European Union and the United States each both only have three graduate level degrees offering Threat Analysis and Management courses, whereas at undergraduate level, the United States has one university offering courses on Threat Analysis and Management, while European Union has none.

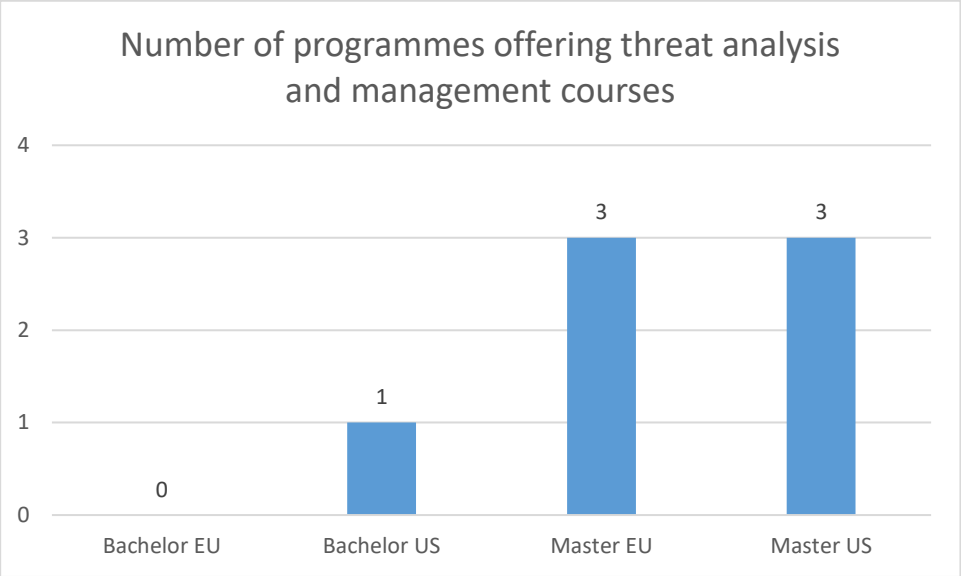


Figure 46. Number of degrees with Threat Analysis and Management courses

Examination of courses in degree programme curriculums clearly shows a lack of Threat Analysis and Management courses across all educational levels and geographical regions. As stakeholders highly value Threat Analysis and Management skills, universities are unable to equip the students with the skills to meet the demand by stakeholders.

Programming, Incident Handling and Response, Digital Forensics and Cloud Security

Programming, Incident Handling and Response, Digital Forensics and Cloud security received equal amount of responses for the question of which skills respondents would now improve. Programming categorization, courses and course natures were covered in Programming subsection of Chapter 5.2.1, Incident Handling and Response subsection of Chapter 5.2.1 and Digital Forensics subsection of Chapter 5.2.1.

As seen in Figure 47, all Cloud Security courses available across universities in European Union and the United States fall under the Operate and Maintain category of NCWF. While the number of available courses is low, making trend analysis more difficult, graduate level degrees seemed to have more availability for Cloud Security courses in both the United States and European Union. At undergraduate level degrees, the United States only had one degree which offered a single Cloud Security course. A total of four Cloud Security courses were available for European Union undergraduate level students.

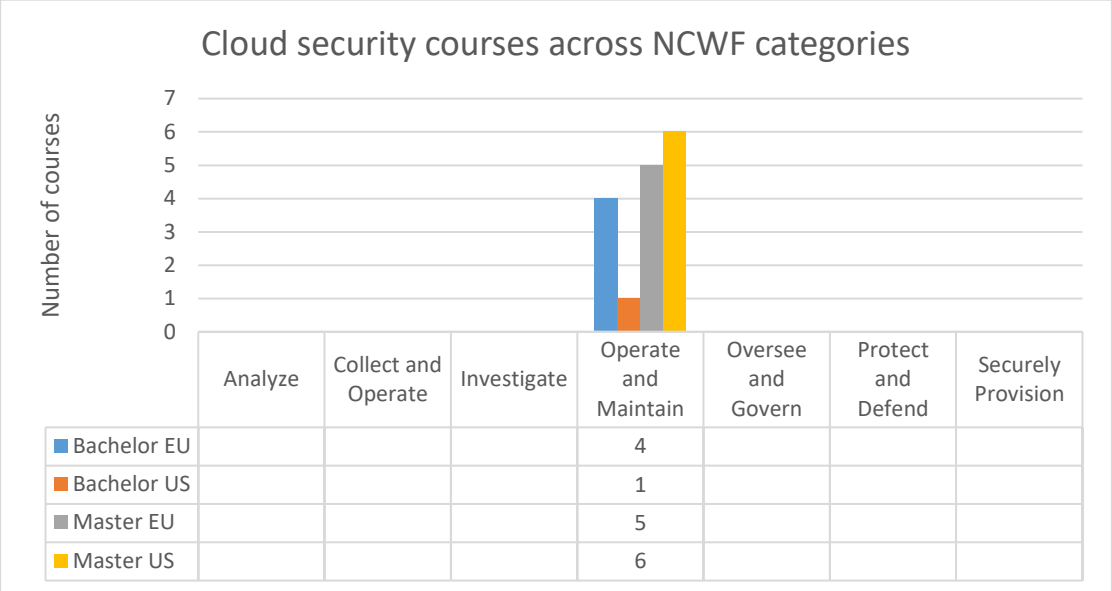


Figure 47. Categorization and number of courses in Cloud Security

European Union based universities seem to lean more towards mandatory courses in this area of expertise, while the United States chooses to provide elective courses, as expressed in Figure 48. However, due to the relatively small number of courses, determining trends across education levels and geographical areas is difficult.

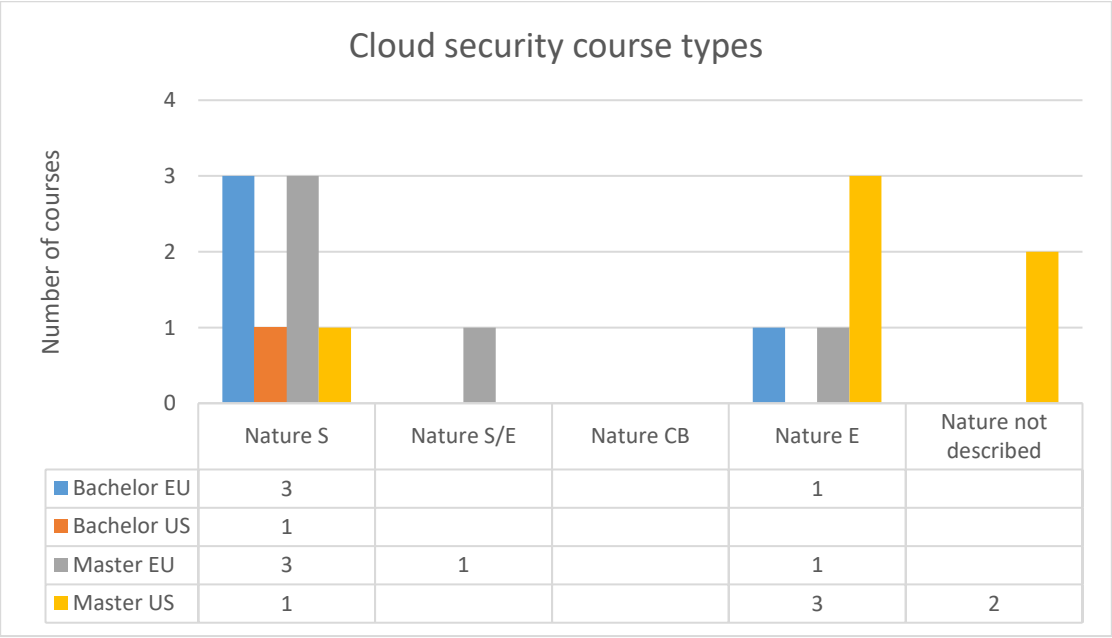


Figure 48. Number of Cloud Security courses across course types

Figure 49 shows the distribution of Cloud Security courses across the 14 programmes. Noticeably small availability is at undergraduate level degrees in the United States, with only a single university offering a course in Cloud Security. Only 14 of total of 69 degree programmes offer direct courses in Cloud Security, and the availability of the courses is poor in terms of percentage of degrees when compared to, for example, availability of networking courses.

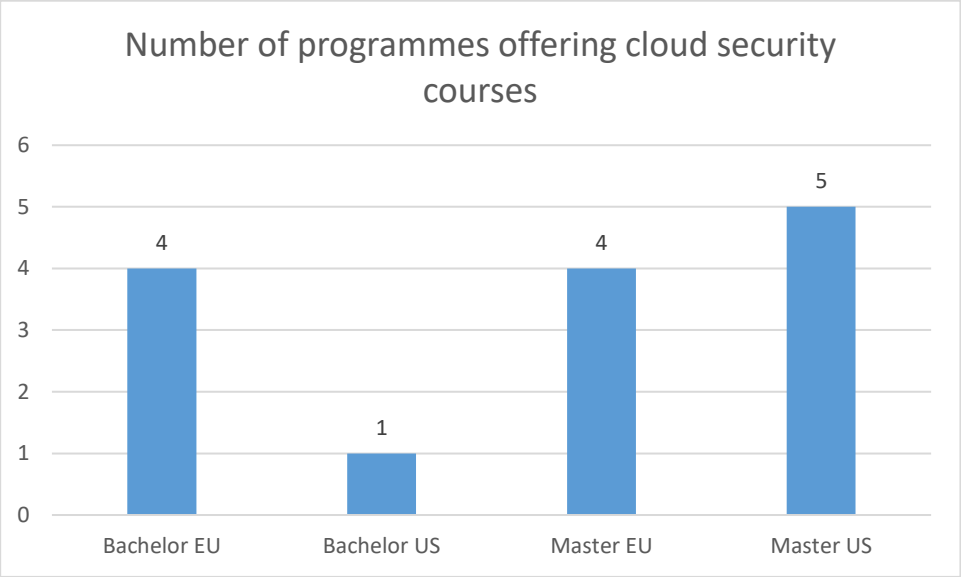


Figure 49. Programmes offering Cloud Security

Cloud Security was not covered in the chapter processing the most important areas of expertise, as cloud related skills received only one response in the questionnaire. This indicates that that the area of expertise is not among the most important areas of expertise, demand for the expertise exists, nonetheless.

5.2.3 Comparing curriculum data data to questionnaire respondents' perceived areas of expertise often missing from recruits

Respondents working in a recruiting position were asked to list skills which were most often lackluster among job applicants. The purpose of the question is to provide universities data that can be used to identify missing areas of expertise in the

curriculum and to analyze why skills are lacking even if courses are available in those areas of expertise. Familiar areas of expertise, such as Networking and Programming, made their way high up in the list of answers again, reinforcing the view that these might warrant closer investigation.

Soft Skills

The most common area of expertise missing among the recruits was the same as in most important areas of expertise in cyber security – Soft Skills. Soft Skills include skills such as communication, comprehension, teamwork, problem solving and critical thinking abilities. These skills are usually learned as a part of other courses or projects, or during projects and tasks at work, and are rarely taught directly. As education targeting soft skills specifically is rarely provided by the universities, or may be difficult to provide as standalone courses, improving soft skills in new recruits could be achieved by exposing the students to challenges requiring more advanced soft skills through other courses.

Technical Capabilities

Technical Capabilities received the second most responses in the questionnaire. Technical Capabilities in this chapter refer to Operating Systems, Server Roles and Applications, for which the course data has been previously covered in subsection with the same name in Chapter 5.2.1. Respondents felt that candidates often have underwhelming technical skills or do not understand the technologies used. When compared to available courses in the degree programmes, the expertise should not be an issue. This indicates a challenge in getting the current supply of education to match the demand for expertise, but the specific nature of the skill gap should be studied further to determine the exact cause and steps required to match the education and need for expertise. The root cause for the mismatch could vary from the content of specific courses available not being relevant after graduation, lacking depth of courses, to the students lacking skills to apply what they have learned at work.

Networking

Third area of expertise in the responses was Networking. Respondents felt that especially understanding enterprise networks and their complexity and interdependencies is often missing among the candidates. Networking courses were covered in Networking subsection of Chapter 5.2.1, and when comparing perceived need for more Networking education to the availability of Networking courses in degree programmes, the issue why candidates seem to miss the necessary skills is not the availability of the courses, but rather the lacking depth of the courses.

Programming

Programming skills were also often found to be missing among the candidates. As with Technical Capabilities, the programming skills were often underwhelming, or programming languages, software or software architecture were not understood well enough. Offering of the programming courses was covered in Programming subsection of Chapter 5.2.1, as programming was also one of the most important areas of expertise in cyber security. Course curriculum analysis suggests that the availability of courses in degree programmes is good at all levels of education, as well as in both examined geographical regions, which would indicate that the cause of the skill gap is a result of course contents, depth or application of knowledge, and should be studied further.

Threat Modeling

Threat Modeling capabilities also received several responses from the questionnaire respondents as skills that needed improvements in new recruits. Threat Analysis, Modeling and Management was covered in a subsection of Chapter 5.2.1, and the offering of the courses was found to be very low. Threat modeling could be embedded to risk management courses as well, but according to the offering of courses within collected course data and questionnaire responses in missing skills among the candidates, the depth of courses is too shallow and availability too low.

5.2.4 Comparing course data to skills requiring more attention at the start of career

Questionnaire respondents were also asked what skills the respondents were missing, or which skills should have been stronger, at the start of their career. The aim of

this is to gain a better view at whether the areas of expertise in demand have changed, or if these follow those that current recruit candidates are missing. Using the reviewing scope determined in Chapter 5.1, the reviewed items in this chapter are limited to five areas of expertise that received the most answers. Programming, Soft Skills, Networking and Technical Capabilities have already been covered in earlier chapters and thus have not been reviewed again. However, the second most responses were given to Business Management, which has not been covered previously.

Business Management

Figure 50 shows how majority of the Business Management courses covered in collected data do not fit in the NCWF categorization as the focus of the courses is outside cyber security domain. The more managemental courses, such as New Jersey Institute of Technology's course "Information Technology, Business and the Law", land in the "Oversee and Govern" category of NCWF, while a few other courses fit better in "Securely Provision" Category of NCWF.

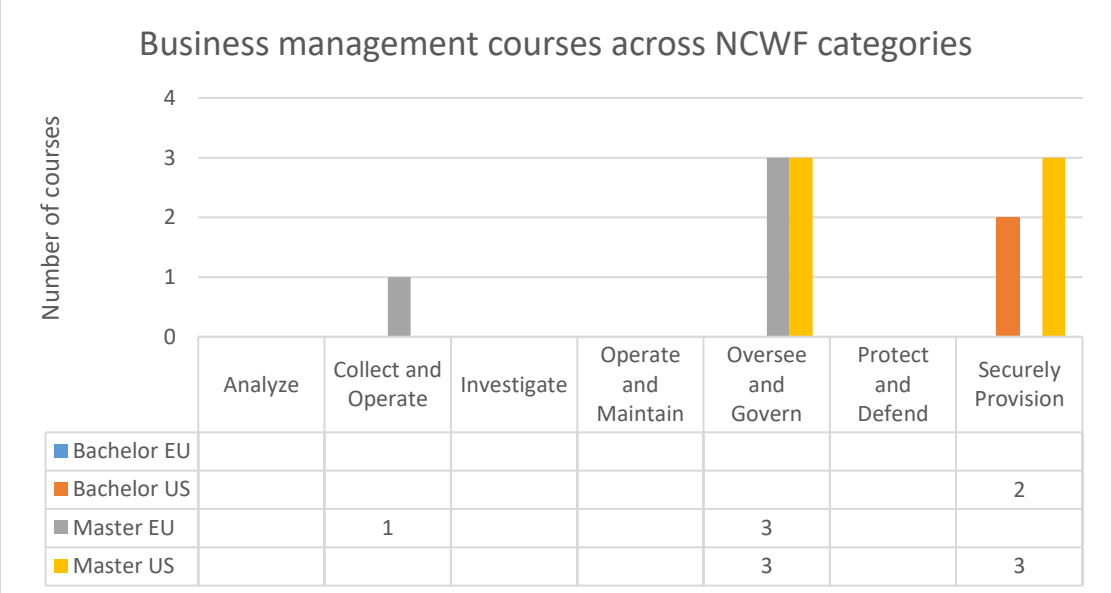


Figure 50. Number of Business Management courses across NCWF categories

The nature of Business Management courses varies across study level and geographical region, with a significant number of elective Business Management courses offered for the United States based graduate level students, as shown in Figure 51.

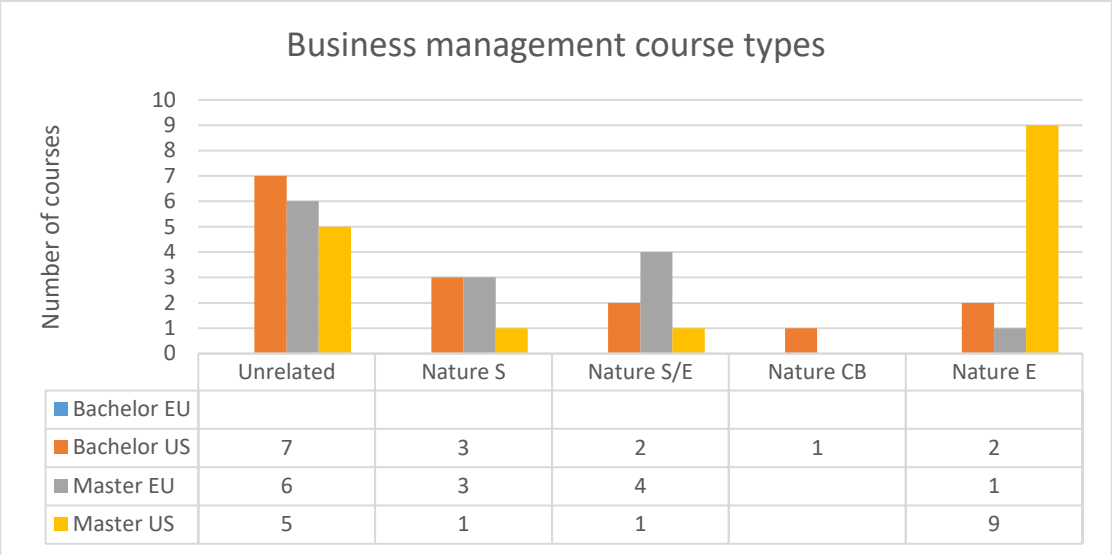


Figure 51. Number of Business Management courses across course types

It is noteworthy to mention that, as seen in Figure 52, no Business Management courses are available at undergraduate level in European Union based universities, or the relevant studies have been embedded in other courses, such as Entrepreneurship courses. Courses are available at some universities at both examined education levels in the United States, and at graduate level in European Union, but not at undergraduate level for European Union students.

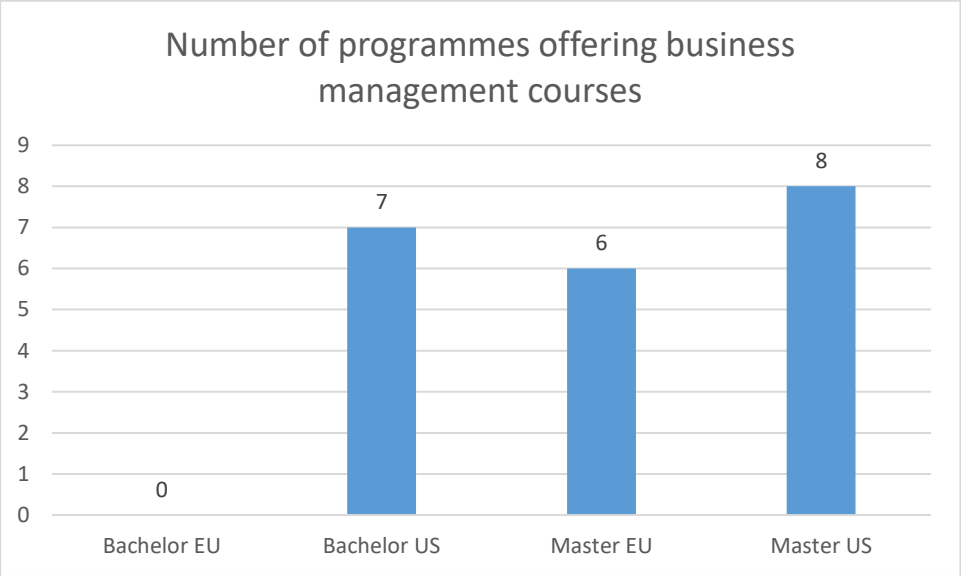


Figure 52. Programmes offering Business Management

5.2.5 Overall comparison of curriculum data and questionnaire results

The comparison of questionnaire responses and collected curriculum data provided several observations worth of notice. Stakeholder responses indicate that cyber security professionals require a proper understanding in networking and programming skills, as well as broad capabilities in technical expertise. Stakeholders also value soft skills, and to succeed in cyber security, personality and behavioral traits are significant.

Comparing the stakeholder responses to course offerings in universities, indicates a good availability of courses in networking, programming and technical expertise. However, as stakeholders have responded, the recruit candidates are often underperforming in these same categories. This indicates a mismatch between education and demand for expertise, which may be a result of the courses not being in-depth enough to answer to the demands, or perhaps challenges in applying the learned skills in real-life scenarios.

Incident Response, Education and Training, Log and Security Analysis and Threat Analysis and Management areas of expertise faced a different challenge, as courses were not easily available at different education levels. According to insight obtained

from the collected data, the offering for such courses does not meet the current demand for the expertise provided for them.

Penetration testing was considered by the questionnaire respondents to be an important aspect of cyber security, as well as a skill which they were highly interested to improve. Offering of penetration testing courses could be higher, however stakeholders did not indicate penetration testing as a skill for which the recruit candidates' abilities were underwhelming. This could be explained with the underwhelming skills in technical capabilities, as if person lacks in technical capabilities, the person most likely is not performing well in penetration testing either.

Cloud Security was not ranked in the most important areas of expertise but was ranked among the areas of expertise that the current workforce wanted to learn. The availability of the courses is low, which may pose an issue in the future, considering that cloud services are presently becoming more common across all fields.

The comparison of response data and curriculum data is used to answer the research questions, "does the current cyber security education fulfil the demands of different stakeholders" and "do the stakeholder demands match the current curriculums of cyber security education?" For both questions, answer is partially yes, as well as no. The course availabilities for most of the important areas of expertise are fulfilled well, however stakeholders still feel that new recruits often underperform in the same areas of expertise. On the other hand, some demands for expertise did not meet the availability of courses on the same level, for example availability in Incident Response, and Education and Training. The results indicate that courses with availability are not filling the area of expertise's in-depth demands, and courses without availability result in graduating cyber security students missing the necessary skills in demand. Additional research into course depths would provide a more comprehensive answer to the research questions, as course descriptions were mostly left out of scope for the current study.

5.3 Cyber security workforce profile

Questionnaire respondents were asked several different questions regarding their backgrounds, the answers to these were analyzed in Chapters 5.1.1 to 5.1.8. As a result of data analysis, the profile described below could be created with the response data.

34 out of 50 degree programmes obtained by questionnaire respondents were based either in non-cyber security ICT or cyber security. As covered in Chapter 5.1.4, if respondent had multiple degrees, all degrees were included in response data. Respondents' industry of employment is most commonly ICT and Telecommunications (64% of respondents) at a private sector organization (64% of respondents). The overall respondent is active and willing to educate themselves by attending cyber security events, courses or by certifications, as 93,2% of respondents had taken part at least of one of these. Work distribution across respondents covered the full spectrum from purely managemental to purely technical roles, including a mix of both aspects, with 56% of respondent job titles implying technical expertise. The respondents' median career duration in cyber security is 2-5 years with a median overall ICT career duration of 5-10 years.

5.4 Expertise profiles of degree programmes and stakeholder demands

Expressing the curriculums and stakeholder demands as a radar charts allows for a clearer picture of the curriculums, with more noticeable anomalies in NCWF category distribution of courses. NCWF category numbers have been used as radar chart focal points instead of complete names, the equivalency table for NCWF category numbers and names is listed below in Table 3.

Table 3. NCWF category number and name equivalencies

Category number	**Category name**
1	Analyze
2	Collect and Operate
3	Investigate

4	Operate and Maintain
5	Oversee and Govern
6	Protect and Defend
7	Securely Provision

Figure 53 shows the course NCWF distribution for degree programmes with length between 160 to 190 ECTS in EU undergraduate level. It is noticeable, that three of the curriculums differ from the rest of the data. Most of the other degree programmes tend to lean towards NCWF categories “Operate and Maintain” “Securely Provision”. Noroff school of Technology and Digital Media provides two cyber security degrees for their students, one focusing in core cyber security, and another focusing on digital forensics, expressed in green and blue in the Figure 53. Noroff’s Bachelor in Digital Forensics programme focuses on digital forensics, which falls under the NCWF category “Investigate”. Noroff' second degree programme on Cyber Security consists of courses emphasizes NCWF “Protect and Defend” category, differing from most other undergraduate degrees in cyber security within this scope. Additionally, the degree programme in Czech Technical University of Prague holds a stronger focus towards NCWF “Securely Provision” Category, as the majority of courses fall under Programming and software development, which land under the NCWF “Securely Provision” Category.

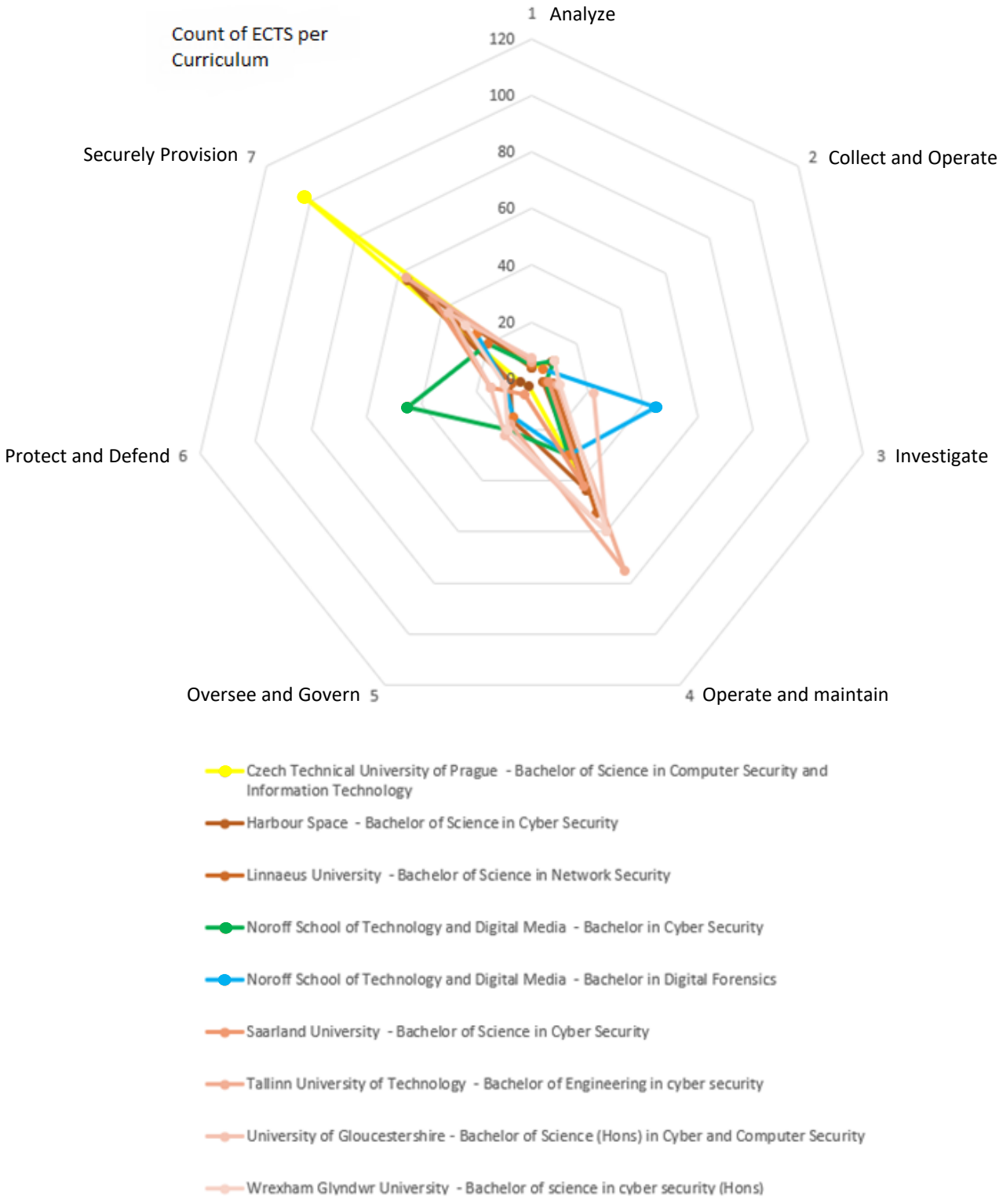


Figure 53. Sum of ECTS of European Union based universities' undergraduate courses in each NCWF category

Degree programmes with length between 191-220 ECTS only consist of a single degree programme, as shown in Figure 54. The weighting of the curriculum follows

other cyber security degree programmes, where majority of courses fit in “Operate and Maintain” category of NCWF and “Securely Provision” category of NCWF “Securely Provision”. The curriculum consists mainly of technical and programming courses, most technical courses are in NCWF “Operate and Maintain” category, while most of the programming courses are categorized in NCWF “Securely Provision” category, resulting in a distribution similar to most other cyber security degree programmes.

Figure 54. Sum of ECTS of European Union based universities’ undergraduate courses in each NCWF category

The degree programmes with a length of 221 to 240 ECTS follow a similar pattern in weightings in NCWF categories as the shorter degrees, shown in Figure 55. The main emphasis of the curriculums is between NCWF categories “Operate and Maintain” and “Securely Provision”.

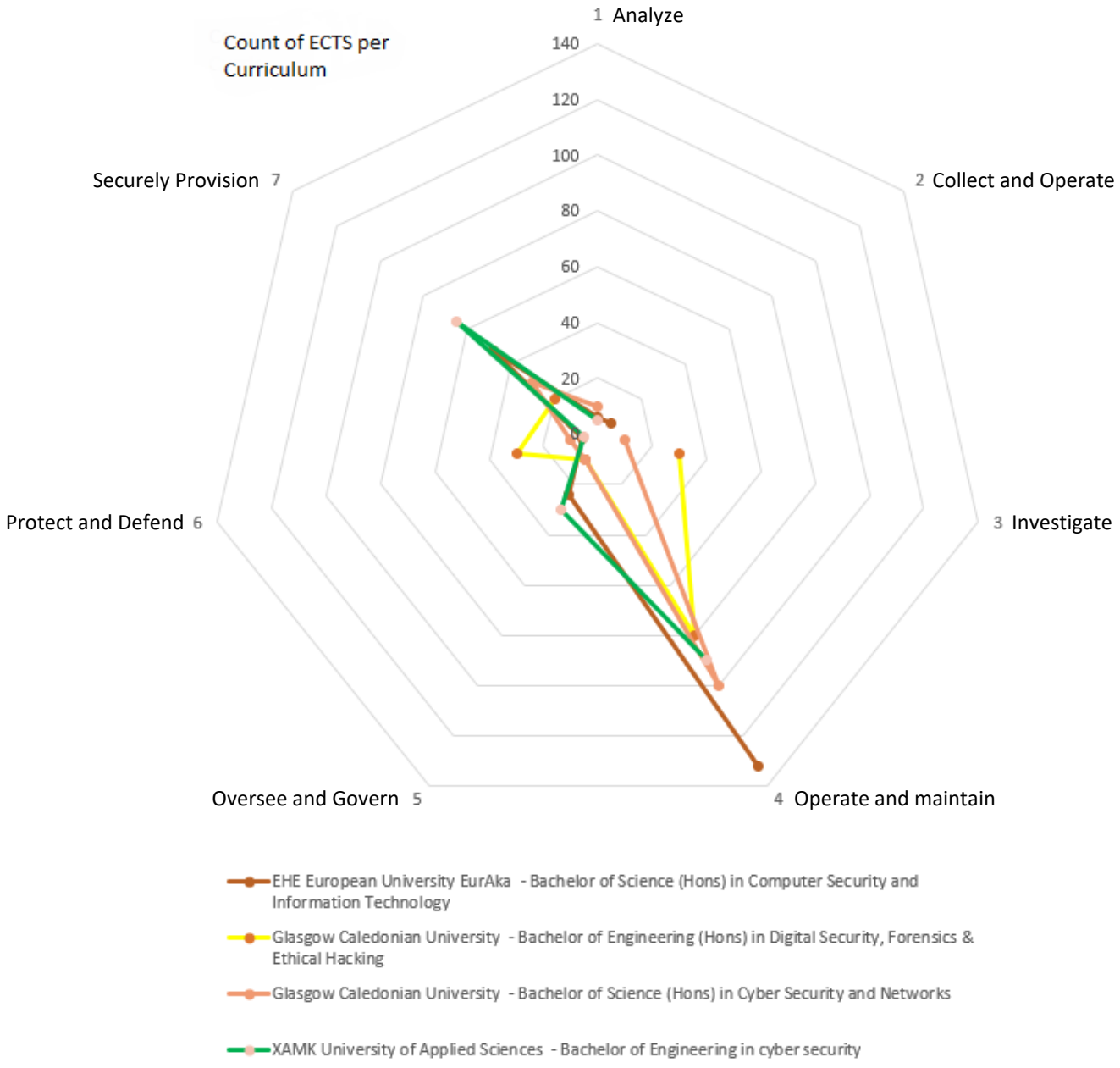


Figure 55. Sum of ECTS of European Union based universities’ undergraduate courses in each NCWF category

In the United States, the variation of degree programme length is smaller in undergraduate degree programmes. One single degree programme is in 160-190 ECTS scope and the remaining degree programmes are between 221-240 ECTS.

Degree programme curriculums have more variation in NCWF category weightings in the United States than in European Union. Figure 56 shows that most focus still appears to be in NCWF categories “Operate and Maintain” and “Securely Provision”, but the degrees do not follow each other as closely as in European Union. This variation may be explained by more focused degree programmes in some areas, for example, Slippery Rock University’s BSc in Cyber Security with Security Governance degree programme consists of large number of courses in NCWF “Oversee and Govern” category, such as policies and governance courses. When compared to European Union degree programmes, the most noticeable difference is the emphasis on NCWF “Oversee and Govern” category, with two degree programmes offering a fair amount of courses in the category.

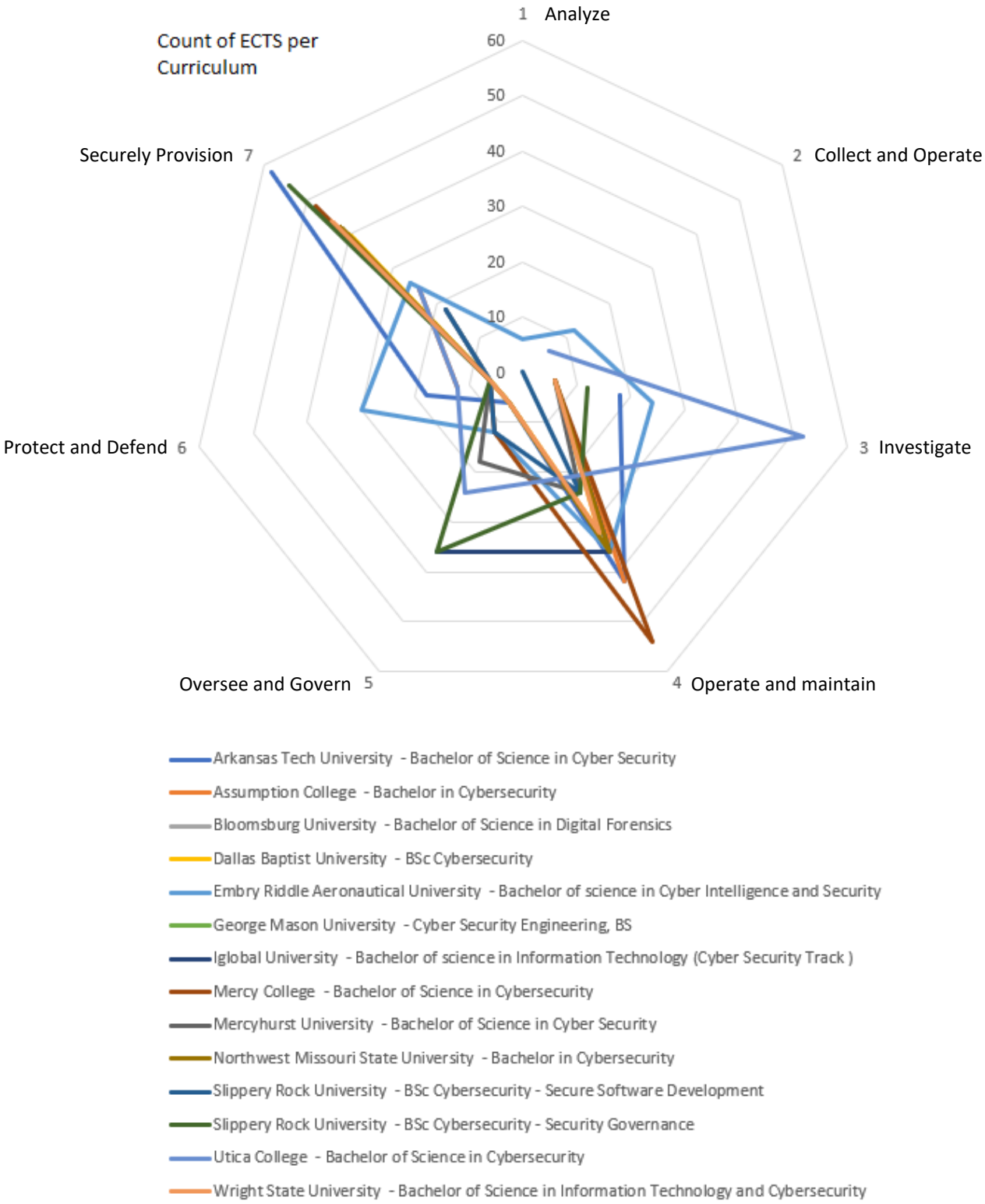


Figure 56. Sum of ECTS of the United States based universities' undergraduate courses in each NCWF category

The single degree in 160-190 ECTS category follows a similar format as most other cyber security courses, with heavy focus on NCWF categories “Operate and Maintain” and “Securely Provision”, as seen in Figure 57.

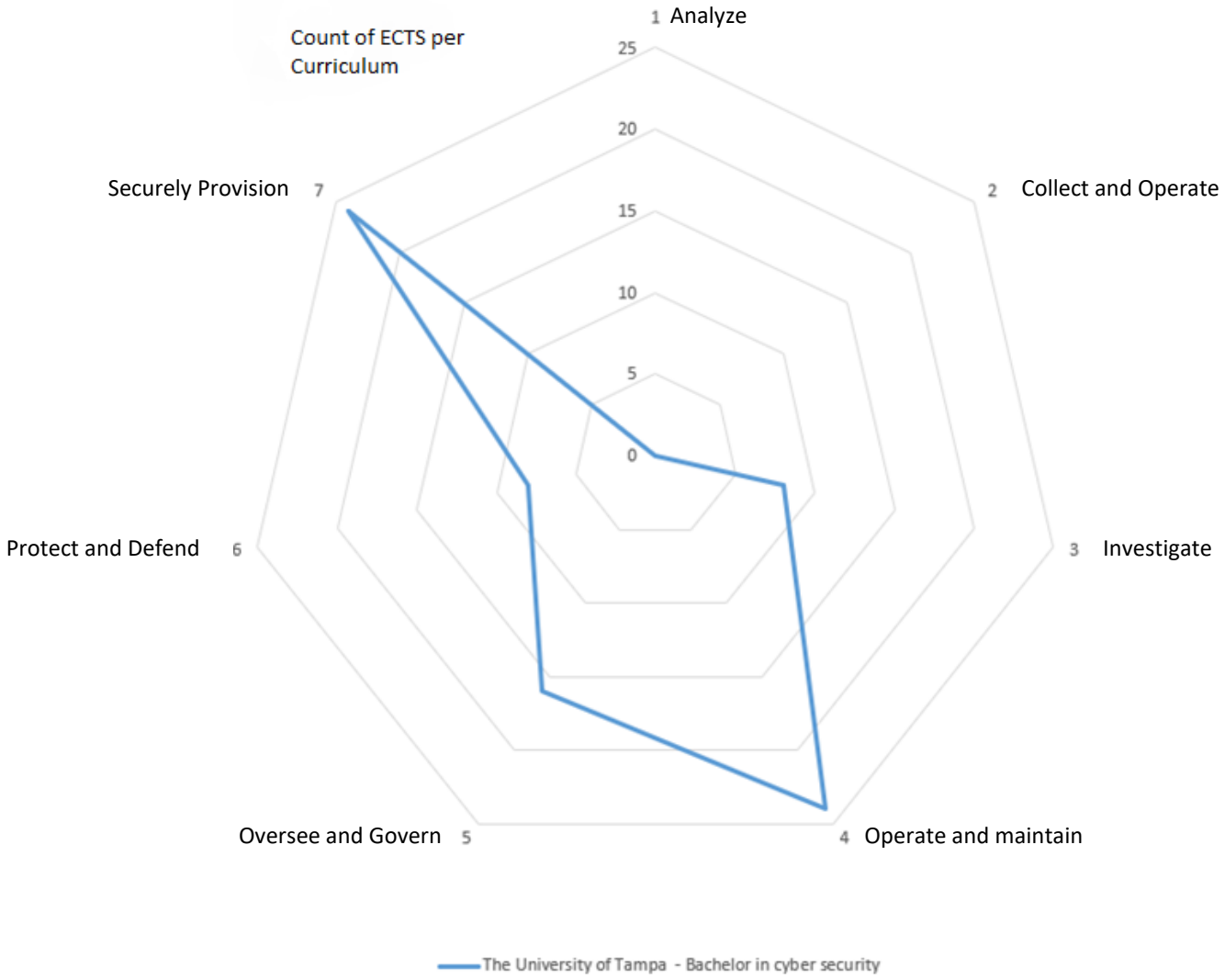


Figure 57. Sum of ECTS of the United States based universities’ undergraduate courses in each NCWF category

When analyzing graduate level degrees in European Union with 86-110 ECTS scope, the variation in NCWF category emphasis is higher than in undergraduate degrees. This indicates that degree programmes are more specialized in some areas, even when the title for most degrees is the same. The main emphasis still is in the NCWF categories “Operate and Maintain” and “Securely Provision”, however Figure 57 also

shows additional emphasis on the other categories, such as NCWF “Collect and Operate” category. Compared to undergraduate level degrees, courses in NCWF “Collect and Operate” category are not as readily available in graduate level degrees.

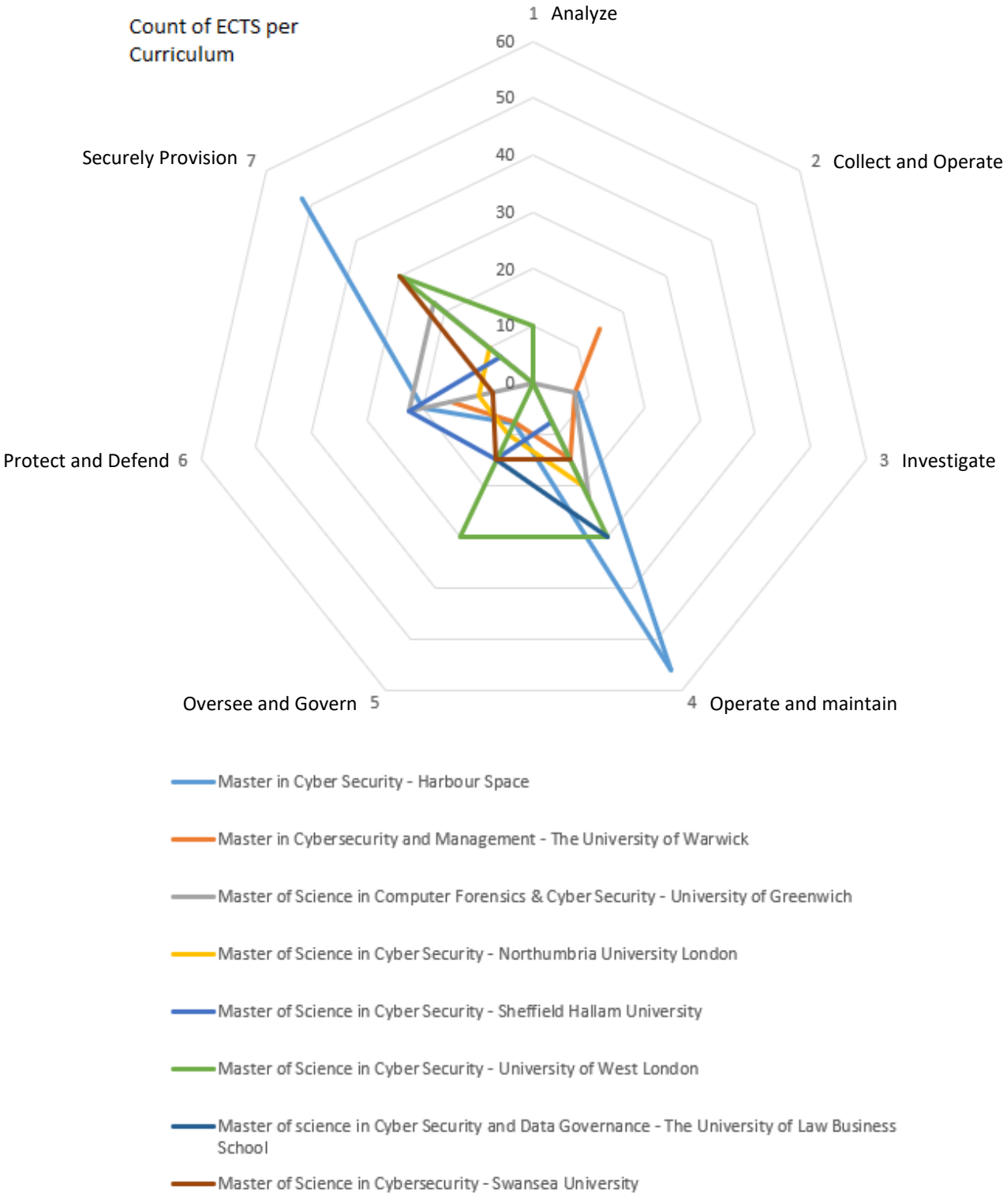


Figure 58. Sum of ECTS of European Union based universities' graduate level courses in each NCWF category

When comparing graduate level curriculums in European Union based universities curriculums, Tallinn University of Technology's degree programme stands out from the rest. This is caused by modularity of the degree programme, as the degree programme has multiple different cyber security related modules from which students choose one. This causes an error in expression of data in the number of courses provisioned, as more courses are available for students than they can enroll in. Rest of the degrees are similar in terms of emphasis, with focus on NCWF "Operate and Maintain" category and "Securely Provision" category, with a small deviation in NCWF "Oversee and Govern" category in degree programmes provided by University of Turku, as the programme includes fair amount of studies in the NCWF "Oversee and Govern" category, shown in Figure 59.

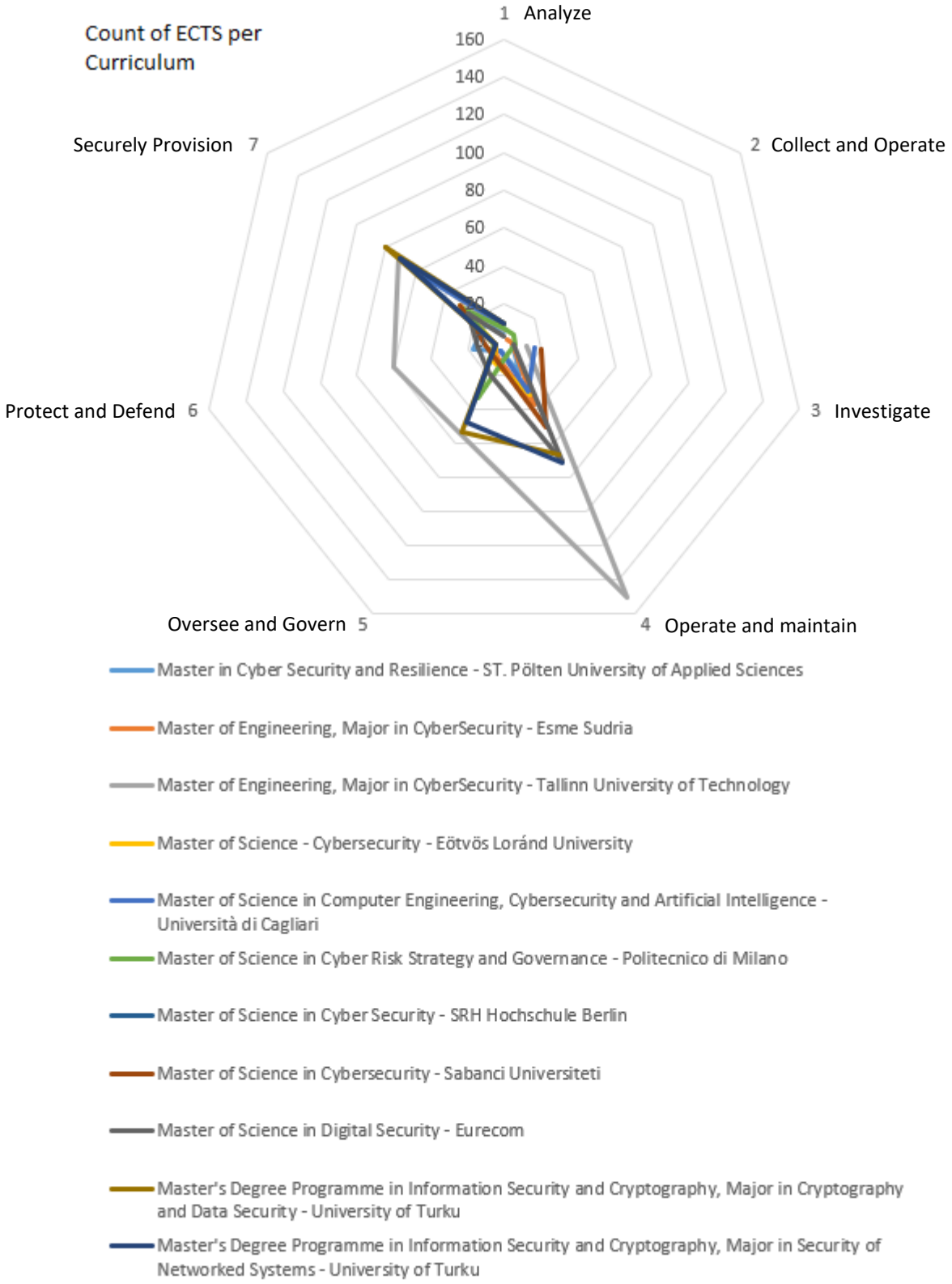


Figure 59. Sum of ECTS of European Union based universities' graduate level courses in each NCWF category

In the United States, all graduate level degrees fall under 60-85 ECTS in terms of duration. Majority of the curriculums have similar emphasis as European Union graduate degrees, with focus on NCWF “Operate and Maintain” category and “Securely Provision” category, as shown in Figure 60. Some degree programmes have more specialized curriculum, setting them apart from the rest of the degrees. Examples from these degree programmes include SANS Technology Institute’s Master of Science in Information Security Engineering with major weighting in NCWF “Protect and Defend” category, expressed with light blue in Figure 60, and Tufts University’s Master of Science in Cyber Security and Public Policy, expressed in light green in Figure 60, with weighting in NCWF “Oversee and Govern” and “Securely Provision” categories.

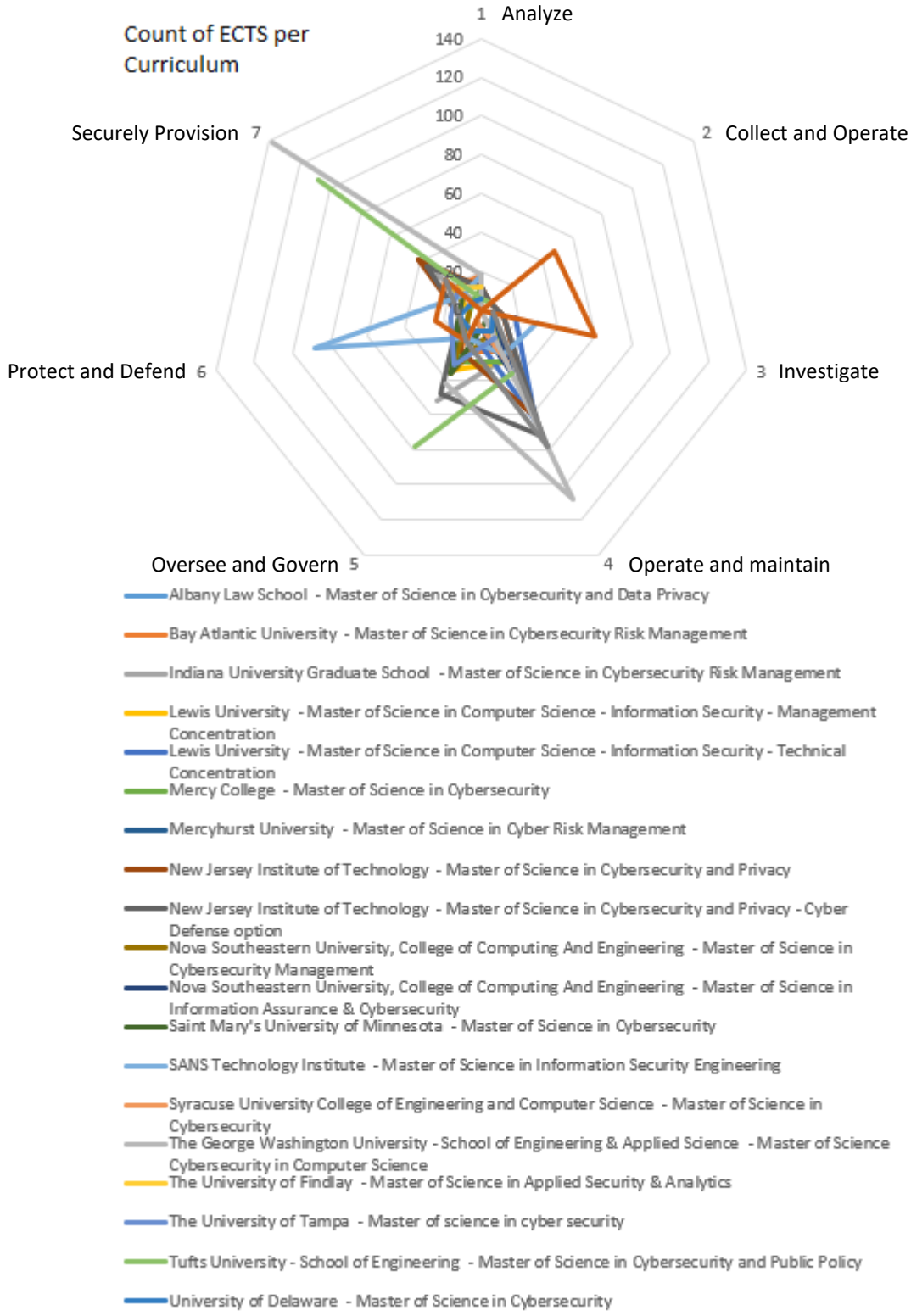


Figure 60. Sum of ECTS of the United States based universities' graduate level courses in each NCWF category

Questionnaire response data was also crafted as radar charts to allow displaying of curriculum data and questionnaire response data in radar expressions. Figure 61 expresses what the respondents view as the most important areas of cyber security in terms of NCWF categories, with greatest amount of responses landing on NCWF “Operate and Maintain” Category. This includes the often-mentioned basic operations in ICT, such as Networking. Second most responses land on “Oversee and Govern” category, which includes the more managemental areas of expertise in cyber security, such as end user education and training. Third most answers landed on NCWF “Securely Provision” category, including skills such as programming and risk management. “Protect and Defend” category related answers were fourth at a small margin, consisting of areas of expertise that are specialized especially towards cyber security testing and cyber resilience enhancements, such as Penetration Testing. Figure 61 contains answers from all NCWF categories, not only the answers limited with the scoping in Chapter 5.1.

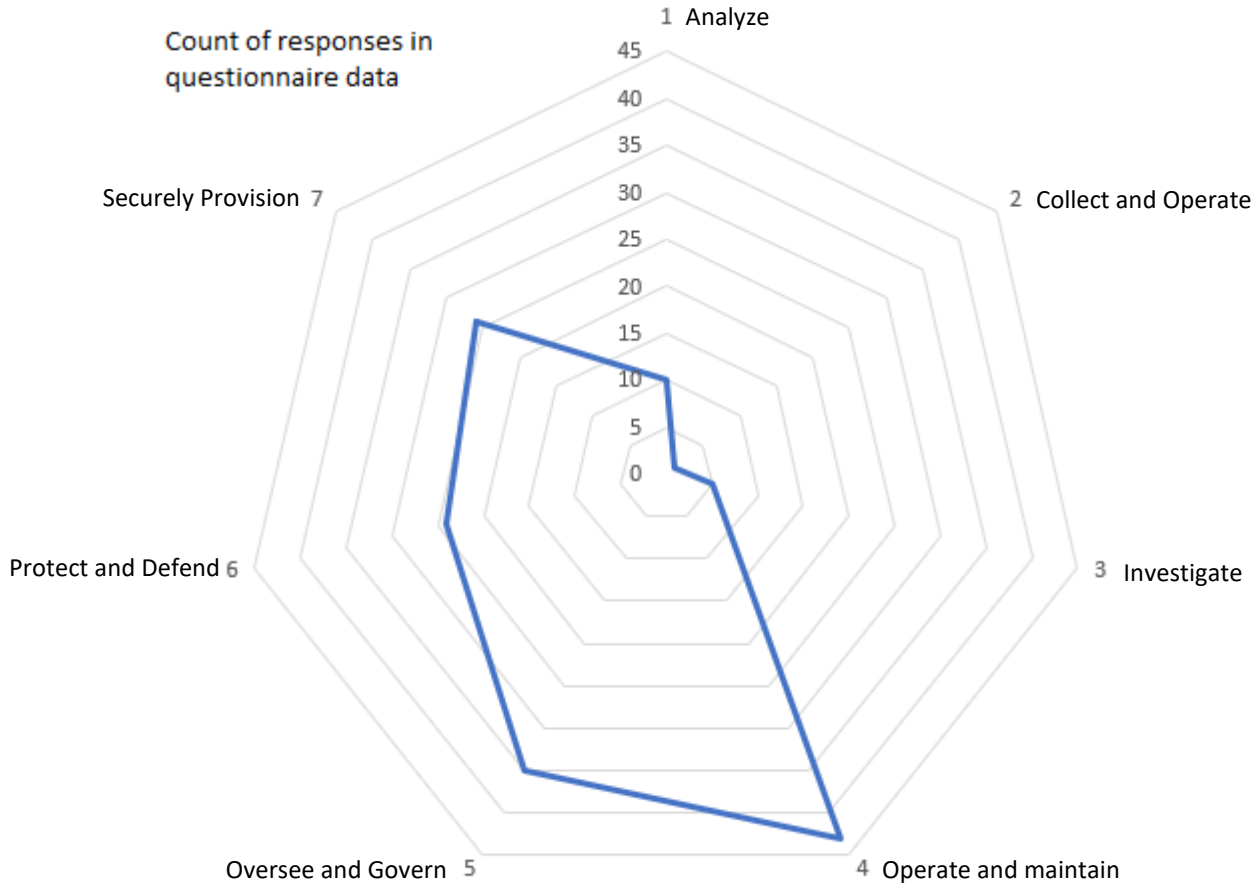


Figure 61. Number of answers to important areas of expertise identified by questionnaire respondents in each NCWF category

The categories where respondents would like to increase their expertise partly follow same pattern, as with the most important areas of expertise, the main emphasis is still on NCWF "Operate and Maintain" category with a fair share of responses falling under "Securely Provision" category and "Protect and Defend" category, as seen in Figure 62. However, NCWF "Investigate" category has received more responses in contrast to previous questions. This indicates that either the need or interests in analysis skills has increased across the stakeholders. NCWF "Operate and Maintain" category still receiving the most responses is likely due to evolution of technologies, as operating systems and network devices are constantly developed, increasing the need to update current expertise as new features or systems are introduced. A similar evolution is occurring at NCWF "Securely Provision" category, as programming falls under the category, and for example, as programming language frameworks and

technologies are updated or upgraded, the expertise itself also needs updating. Interest in penetration testing area of expertise is shown with high response count in NCWF “Protect and Defend” category.

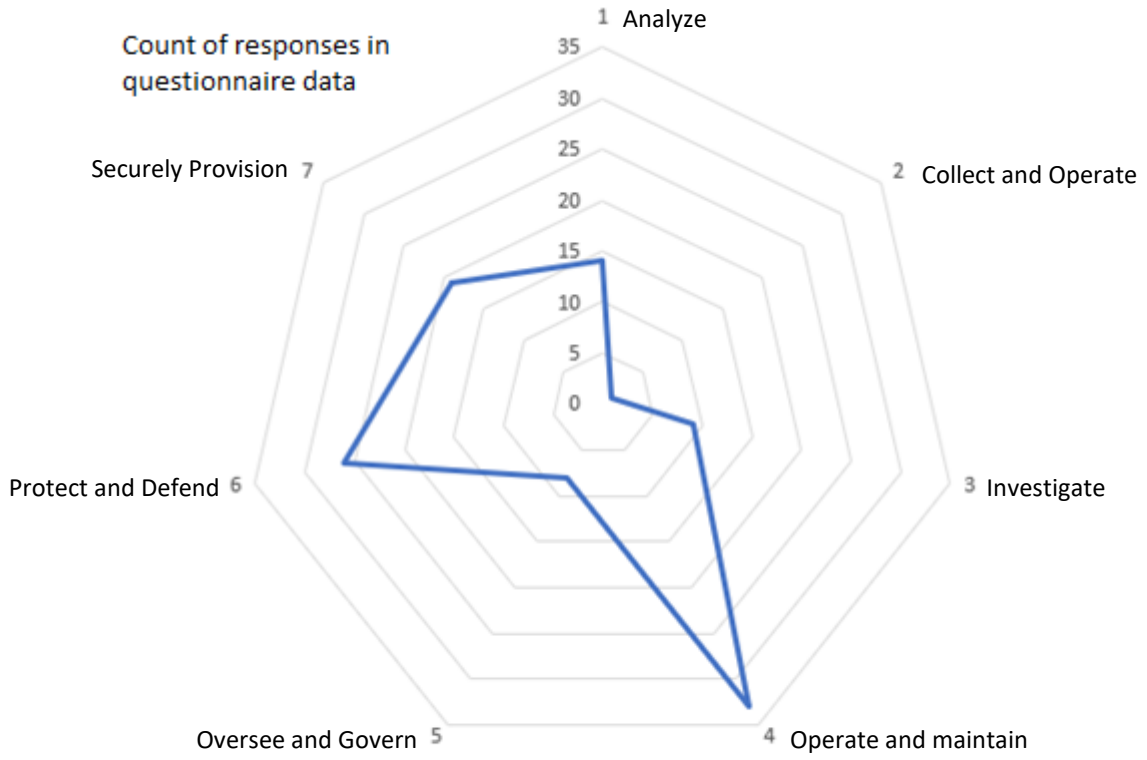


Figure 62. Number of answers to areas to improve identified by questionnaire respondents in each NCWF category

As Figure 63 shows, majority of the responses for lacking abilities in new recruits are categorized in NCWF “Operate and Maintain” category and “Securely Provision”. The emphasis follows an expected pattern, as the missing skills identified in Chapter 5.2.3 mostly land in Networking and Technical Abilities, which are included in NCWF “Operate and Maintain” category, or Programming, which is a part of NCWF “Securely Provision” category. The distribution of the results could have been wider if the respondent pool sampling were larger, as only 31 of 44 respondents were in a recruiting position.

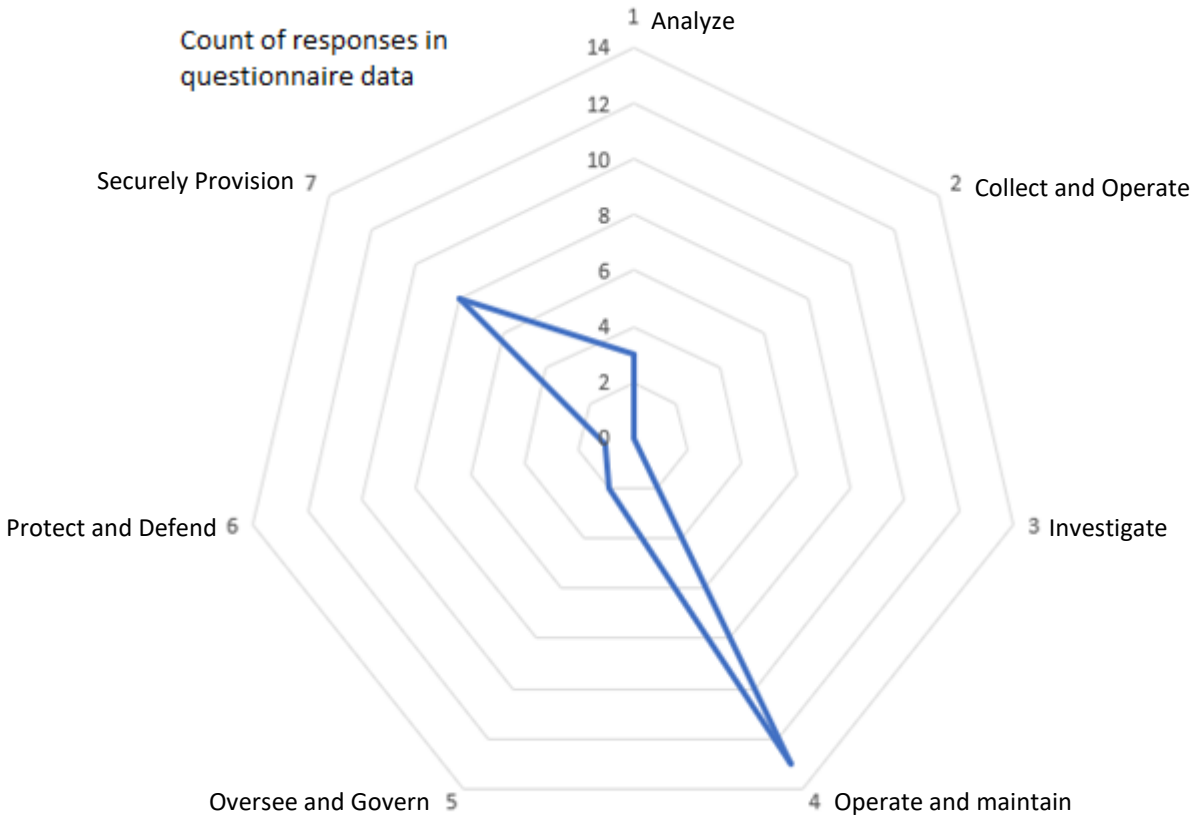


Figure 63. NCWF categories where respondents felt the recruits were missing skills

Respondents were also asked which skill they would have improved at their start of their career to perform better at their work. Analysis of the responses shows a deviation from previous categorizations. In earlier analyses from the respondent data, NCWF “Operate and Maintain” category has been dominant in the responses. However, NCWF “Securely Provision” category received the highest number of responses, as seen in Figure 64. The deviation is due to multiple answers in programming related areas of expertise, which falls under NCWF “Securely Provision”.

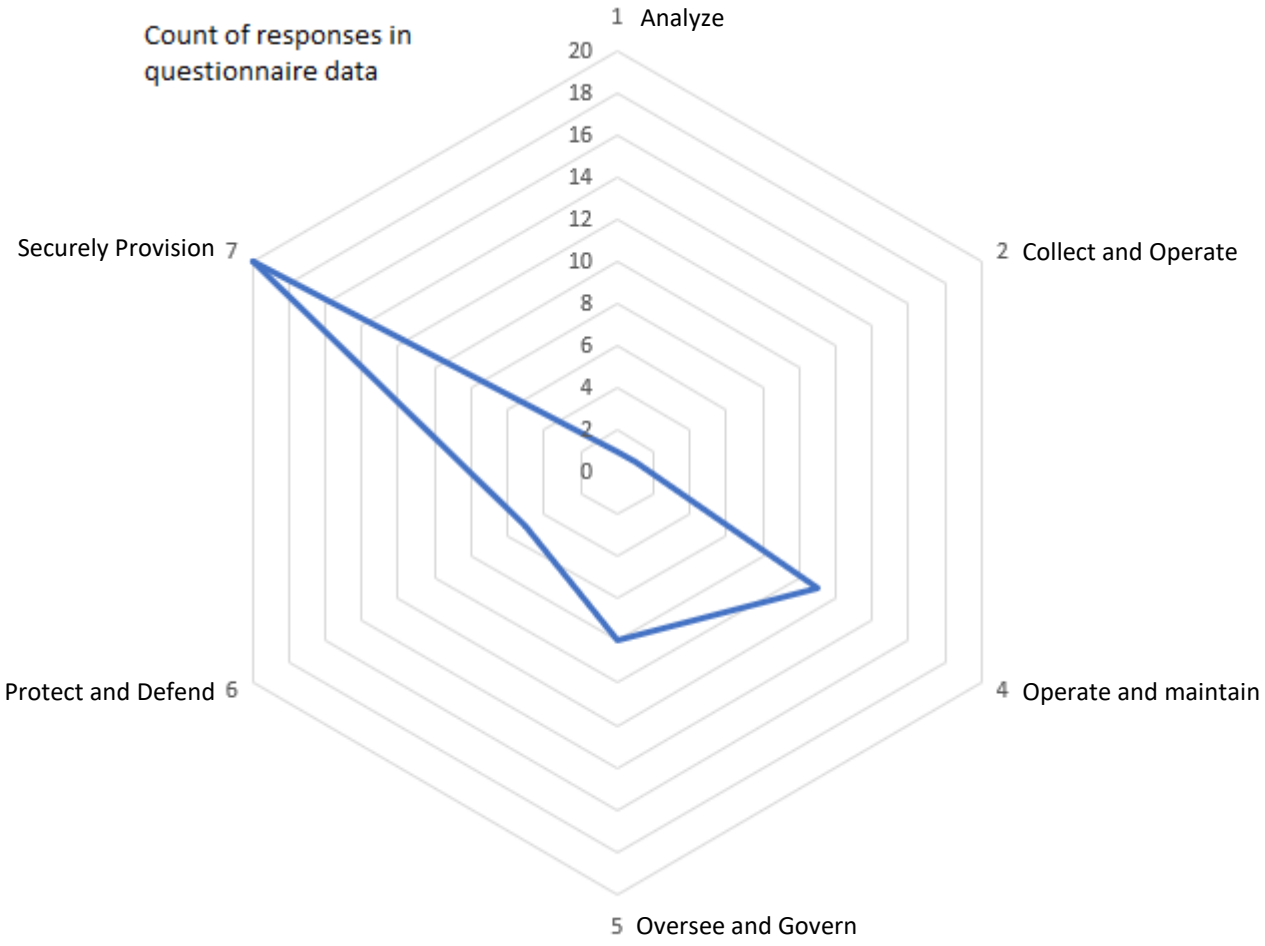


Figure 64. Respondents skills that could be better at the start of career expressed in NCWF radar

While the responses to this question have not been compared to curriculum data, the NCWF category focus distribution is included as additional information to indicate which areas of expertise the respondents felt that would have smoothened the start of their career.

Comparison and analysis of the respondent data and curriculum data shows that majority of curriculums emphasize NCWF “Operate and Maintain” and “Securely Provision” categories. When compared to respondent data, the curriculums seem to answer the demand for these areas of expertise in availability. However, questionnaire responses also emphasis NCWF “Oversee and Govern” and “Protect and Defend” categories as the most important areas where the course availability is not sufficient to meet the demand for expertise, in contrast to NCWF “Operate and Maintain” and

“Securely Provision” categories. Respondents would mostly like to improve their expertise in NCWF “Operate and Maintain”, “Protect and Defend”, “Securely Provision”, “Investigate” and “Analyze” categories. Especially in the case of NCWF “Analyze” category, course offering in curriculums does not meet the demands by stakeholders. Missing skills of recruits falls under NCWF “Operate and Maintain” and “Securely Provision” categories, while analyzing the availability of courses in curriculums indicates that the curriculums would meet the demands of stakeholders.

Overall, the radar expressions are only a tool to express the analyzed data and are not suitable for detailed analysis. The detailed analysis of data comparison in Chapter 5.2 is better suited for this purpose. Universities could improve their own curriculums by dividing the courses into NCWF categories and comparing the relative distribution of courses to degrees provided by other universities and required by stakeholders, possibly revealing areas not included current curriculum or course selection. However, this would also require a more detailed analysis of course contents, and the NCWF categorization alone cannot be used to provide a final answer.

6 Conclusions

Comparison and analysis of the data shows that universities already have a moderately good baseline for Cyber Security degree curriculums, but the curriculums need adjustment in terms of course contents, with possibly a layering on top of networking or programming degree programs. Universities already cooperate with the stakeholders, but based on the research, more in-depth cooperation is needed to fulfil the demands of expertise. By collaborating with the stakeholders, universities could improve their ability to serve stakeholders.

To answer the research question, “Can the contents of cyber security degrees at universities be improved to better meet the demand by stakeholders?”, the answer is yes. After categorizing data into NCWF categories, comparing stakeholder demands and course NCWF category emphasis and course availabilities indicates that the weighting in NCWF categories already are close to that required by the stakeholders, but the issues instead seem to be in the contents of the courses. This indicates that

the technologies, use scenarios or other aspects of the course do not provide the desired skills that stakeholders request.

Open suggestions by questionnaire respondents were covered in Chapter 5.1.12. One of the suggestions was to layer cyber security education on top of a networking or a programming curriculum. Networking and programming were also included in most important areas of expertise as the most underperforming skills in new recruits. Another suggestion was to further specialize degree programmes into more specific aspects of cyber security, such as forensics or cyber security management. Some degree programmes already include such specialized programmes, allowing for deeper expertise within a certain subfield.

The key to improve the curriculums is to listen to the stakeholder demands, however, there are multiple different approaches to fulfilling the development needs. One approach could be to layer the education on top of networking or programming degree, as suggested previously. This would produce specialized experts in cyber security with a strong base knowledge in networking or programming, reducing the issue with underperforming expertise in the networking or programming areas, especially for new recruits. Another approach would be to increase the duration of education and include more advanced courses in networking and programming areas of expertise.

Overall, as the skill gap between stakeholders and employees continues increasing, universities and stakeholders need to collaborate and develop the curriculums together to keep fighting against the threats looming in cyber domain.

7 Development points and discussion

7.1 Development ideas on research

The same research questions can be answered with multiple approaches, and the answers to the research questions might change if the research was executed in more targeted manner. An example of a more targeted research could be comparing and analyzing the quality of network or programming educations in cyber security degree curriculums by, for example, comparing the course descriptions against the

stakeholder collected data to find out which kind kind of expertise is needed in the workforce.

Wider stakeholder questionnaire data sampling could have allowed for a more accurate response data. However, the collected data was sufficient enough to allow for comparison of curriculums and stakeholder demands. The curriculums collected in curriculum data were slightly favoring the United States curriculums, as the United States data included a total of three universities more than European Union curriculums: one at undergraduate and two at graduate level. However, as the research is of high level overview in nature, the slight favor for US curriculums does not generate an inaccuracy that should impact the research results more than marginally.

The curriculum sampling was large and laborious to analyze. Similar research could be more accurate when performed by multiple researchers, as more data could be covered in a shorter amount of time. Applying analysis of course descriptions to curriculum data comparison could provide new insights to the research in the form of including the depth of the courses and provided skill-level, rather than just ECTS-spread. Also, the questionnaire respondent sampling could be larger, and answers could be analyzed separately based on the respondent's role to determine if the demands for skills differ between management and technical individuals.

7.2 Development on the research targets

As a development suggestion for European Union based universities, multiple universities did not include course descriptions in their curriculums when gathering the research data. In worst cases, some universities did not provide course catalogs or course lengths in the degree programme information, or the data was behind student portals. This could create a situation, where a potential student cannot make an informed decision on where to apply to study towards a cyber security degree, as the student cannot be sure what courses are included in the education, or whether the curriculum contains the skills valued by the stakeholders. For the United States based universities, detailed curriculum and course information was available almost without exception.

Analysis of the questionnaire data clearly showed that stakeholders appreciate soft skills. Many of the universities already include research and writing skills in their curriculums, some have team projects and courses which allows some training in collaboration, but in a limited way, as usually the teams are formed inside the class, where the points of interest are similar. This unfortunately does not reflect real life scenarios in collaboration, where the collaborative parties are often from different backgrounds. As a development idea, larger exercises or projects could be executed across students from multiple degree programmes; business management and other degree programme students could be brought together with cyber security students for an exercise that could reflect the different challenges and viewpoints present in real world organizations, and cyber-related actions could be a part of the exercises. This would demand more resources from the university, but could be a more realistic way to train real-life collaboration situations. For the rest of the soft skills, not many universities had courses, for example, in critical thinking or passionate learning subject fields.

7.3 Possible future research ideas based on this research

Previous research with the same setup was not found, though similar research concerning the courses available in universities was available, but without comparison to stakeholder demands. Based on this information, this research provides new research data to the industry. As a pioneer research, additional research with similar setup would provide support to the research methodology and reliability of the research.

Multiple additional research questions developed during the research, in addition to the original research questions, which could create better insight into cyber security education. The first additional research question concerns whether the amount of elective courses in curriculum makes a difference in the cyber security expertise profile of the student. The question could be examined by analyzing whether the student chooses the elective courses by the demands of the potential employers, or are the elective courses chosen by interest towards the expertise area.

Another potential research question has to do with the amount of variation in the course contents in between universities. Research for this could be conducted by collecting data from some scope of expertise included in cyber security curriculums, such as networking courses. The contents of the courses could be then compared to find differences and trends among the courses.

References

About cybersec4europe.Publication on Cyber Security for Europe's website. Retrieved January 23rd from

https://cybersec4europe.eu/about/

Abrams,A. 2019. *Here's what we know so far about Russias's 2016 meddling*. Publication on Time's website. Retrieved January 23rd 2020 from https://time.com/5565991/russia-influence-2016-election/

Alsmadi, I. 2018. *Cybersecurity education based on the NICE Framework: Issues and Challenges.* Referred January 15th 2020 from https://www.isaca.org/Journal/archives/2018/Volume-4/Pages/cybersecurity-education-based-on-the-nice-framework.aspx

Bhadauria, AS. 2016. *Understanding difference between Cyber Security & Information Security*. Publication on Ciso Platform's website. Referred January 20th 2020 from https://www.cisoplatform.com/profiles/blogs/understanding-difference-between-cyber-security-information

Bing,C & Schectman,J. 2019. *Inside the UAE's secret hacking team of american mercenaries*. Accessed 12th April 2020. Retrieved from https://www.reuters.com/investigates/special-report/usa-spying-raven/

Björck, F , Henkel, M , Stirna, J , Zdravkovic, J. 2015. *New Contributions in Information Systems and Technologies*. 1st ed. Switzerland: Springer International Publishing. From: https://link.springer.com/chapter/10.1007%2F978-3-319-16486-1_31

Blackstone, A.2012. Principles of sociological inquiry – *Qualitative and quantitative methods.* Saylor Foundation. Retrieved January 23rd 2020 From https://open.umn.edu/opentextbooks/textbooks/principles-of-sociological-inquiry-qualitative-and-quantitative-methods

Buchy, J. 2016. *Cyber Security vs IT Security: Is There a Difference?*. Retrieved January 20th, 2020 from http://business.gmu.edu/blog/tech/2016/06/30/cyber-securit-it-security-difference/

CA Civ Code § 1798.29. *Accounting of Disclosures.* Retrieved November 12th 2019 from http://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV&sectionNum=1798.29

Cavelty, MD & Egloff, F. 2019. *The Politics of Cybersecurity: Balancing Different Roles of the States*. Zurich: ETH Zurich – Center for Security Studies. From: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3403971

Charlot,F , Amin, F. 2016. *Cybersecurity education challenges and opportunities for academic institutions*. Referred October 3rd 2019 from https://www.linkedin.com/pulse/cybersecurity-education-challenges-opportunities-academic-faisal-amin/

Compare features in Windows Server versions: View the new hybrid,security, and application platgorm features of Windows Server 2019 as compared to previous versions. N.d. Page on Microsoft's web site. Retrieved January 20th , 2020 from https://www.microsoft.com/en-in/cloud-platform/windows-server-comparison

Compare tuition fees schemes in Europe. N.d. Search engine in studyineurope.eu's website. Referred January 20th 2020 from https://www.studyineurope.eu/tuition-fees

Crashoverride: Analysis of the threat to electric grid operations. N.d. Publication on Dragos Inc. Website. Referred October 12th 2019 from https://dragos.com/wp-content/uploads/CrashOverride-01.pdf

Cybercrime Legislation Worldwide.2020. Search engine in United Nations conference on Trade and Development's website. Referred January 20th 2020 from https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Cybercrime-Laws.aspx

Cybersecurity Legislation 2019. 2019. Publication on National Conference of State Legislatures website. Referred October 28th 2019 from www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation-2019.aspx

Das,R & de Guise, P. 2019. *Protecting Information Assets and IT infrastructure in the cloud*. CRC Press.

Di Ciccio, F. 2014. *Comparison of identity theft in different countries.* Referred September 26th 2019 from https://courses.cs.ut.ee/MTAT.07.022/2014_fall/uploads/Main/francesco-report-f14.pdf

Differences between public and private sector cyber security jobs. N.d. Page on Careers in CyberSecurity's web site. Retrieved October 14th , 2019 from https://careersincybersecurity.com/differences-between-public-and-private-sector-cyber-security-jobs/

Digitalisation.N.d. Publication on Finland Ministry of Finance's website. Retrieved January 21st 2020 from https://vm.fi/en/digitalisation

Directive 2013/40/EU. Directive of the European Parliament and of the Council on attacks agains information systems and replacing Council Framework Decision 2005/222/JHA. Official Journal L 218, August 12th 2019, 8. Accessed January 23rd 2020. Retrieved from https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:218:0008:0014:EN:PDF

Elektronisko dokumentu likums. Retrieved November 12th 2019 from https://likumi.lv/ta/en/en/id/68521

Gilles,M. 2019. Five emerging cyber-threats to worry about in 2019. Article on MIT technology review's website. Retrieved April 12th 2020 from https://www.technologyreview.com/2019/01/04/66232/five-emerging-cyber-threats-2019/

HE 177/2016. *Hallituksen esitys eduskunnalle laeiksi opetus- ja kulttuuritoimen rahoituksesta annetun lain muuttamisesta ja välaikaisesta muuttamisesta sekä vapaasta sivistystyöstä annetun lain muuttamisesta*. Referred January 23rd 2020. From: https://www.finlex.fi/fi/esitykset/he/2016/20160177

HE 77/2015. *Hallituksen esitys eduskunnalle laeiksi yliopistolain ja ammattikorkeakoulain muuttamisesta*. Referred January 24th 2020. Retrieved from

https://www.finlex.fi/fi/esitykset/he/2015/20150077

Kaikko, J. 2016. *Focus on the real cyber threat – your end users*. Article on MainSpring's website. Retrieved April 30th 2020 from https://gomainspring.com/cybersecurity-awareness/focus-on-the-real-cyber-threat-your-end-users/

Keane, S. & Reichert,C. 2019. *Huawei says Trump's ban will hurt US 5G deployment*. Article on Cnet.com's website. Retrieved January 23rd 2020 from

https://www.cnet.com/news/trump-effectively-bans-huawei-with-national-security-order/

Kissel, R. 2013. *Glossary of Key Information Security Terms*. 2nd ed. Gaithersburg: National Institute of Standards and Technology. From: https://nvlpubs.nist.gov/nistpubs/ir/2013/NIST.IR.7298r2.pdf

Korkeakouluille uusi rahoitusmalli.2019. Publication on Opetus- ja kulttuuriministeriö's website. Referred January 20th 2020 from https://minedu.fi/artikkeli/-/asset_publisher/korkeakouluille-uusi-rahoitusmalli

Krebs, B. 2016. *Rise of Darknet Stokes Fear of The Insider.* Publication on Krebs on Security website. Retrieved January 23rd 2020 from https://krebsonsecurity.com/2016/06/rise-of-darknet-stokes-fear-of-the-insider/

Kuronen, J & Mansikkamäki, E. 2017. *Introduction to tuition fees, case study: Finnish Universities of applied sciences*. Bachelor's thesis. Oulu University of Applied Sciences, Degree Programme in International Business. Accessed 12th April 2020. Retrieved from https://www.theseus.fi/bitstream/handle/10024/130983/Kuronen_Jenni_Mansikkamaki_Emma.pdf?sequence=1&isAllowed=y

L 681/2010. *Valtioneuvoston asetus tietoturvallisuudesta valtionhallinnossa.* Referred January 23rd 2020. https://www.finlex.fi/fi/laki/alkup/2010/20100681

Lee, D.2019. Adobe is cutting off users in Venezuela due to US sanctions. Referred October 13th 2019 from https://www.theverge.com/2019/10/7/20904030/adobe-venezuela-photoshop-behance-us-sanctions

Lehto,M & Niemelä,J. 2019. *Kyberalan tutkimus ja koulutus Suomessa 2019*. University of Jyväskylä, faculty of information technology. Accessed 12th April 2020. Retrieved from https://www.jyu.fi/it/fi/tutkimus/julkaisut/it-julkaisut/kyberalan_koulutus_suomessa_verkkoversio.pdf

Massacci,F , Sterlini,P , Kadenko, N , Fiebig,T , van Eeten, M.2019.*Governance Challenges for European CyberSecurity Policy: Stakeholders views.* Referred September 27th 2019 from https://cybersec4europe.eu/wp-

content/uploads/2019/11/Governance-Challenges-for-European-CyberSecurity-Policy_-Stakeholders-Views_V.Def_.pdf

McCombes, S. 2019. *How to define your research problem*. Article on scribbr.com's website. Referred January 23th 2020 from https://www.scribbr.com/research-process/research-problem/

McCombes, S. 2019. *Understanding different sampling methods*. Article on scribbr.com's website. Referred January 23th 2020 from https://www.scribbr.com/methodology/sampling-methods/

Mihalcik,C. 2019. *Huawei ban kicks in next week for US government agencies.* Arcticle on Cnet.com's website. Retrieved January 23rd 2020 from https://www.cnet.com/news/huawei-ban-kicks-in-next-week-for-us-government-agencies/

Nakashima,E. 2017. *Russia has developed a cyberweapon that can disrupt power grids, according to new research*. Publication on Washington Post June 12,2017. Retrived October 12th 2019 from https://www.washingtonpost.com/world/national-security/russia-has-developed-a-cyber-weapon-that-can-disrupt-power-grids-according-to-new-research/2017/06/11/b91b773e-4eed-11e7-91eb-9611861a988f_story.html

Payment Statistics 2018: contactless payments have become commonplace for Finns.2019. Publication on Bank of Finland's website. Retrieved January 21st 2020 from https://www.suomenpankki.fi/en/Statistics/payments-statistics/older-news/2019/Payment-statistics-2018-contactless-payments-have-become-commonplace-for-Finns/

Picchi, A. 2018. *Facebook: Your personal info for sale*. Publication on CBS News website. Retrived 23rd January 2020 from https://www.cbsnews.com/news/facebook-your-personal-info-for-sale/

Public Law 113-283-DEC. 18, 2014. *An Act to amend chapter 35 of title 44, United States Code, to provide for reform to Federal Information security.* Retrieved January 23rd 2020 from https://www.govinfo.gov/content/pkg/PLAW-113publ283/pdf/PLAW-113publ283.pdf

Regulation (EU) 2016/679. *Regulation of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data.* Retrieved November 12th 2019 from

https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

Rethinking Strategic Autonomy in the Digital Age. 2019. PDF document on European Commission's website. Accessed on April 12th 2020. Retrieved from https://ec.europa.eu/epsc/sites/epsc/files/epsc_strategic_note_issue30_strategic_autonomy.pdf

Russell, J. 2002. *Trends in information technology and private sector activities*. Article on Sciencedirect's website. Retrieved January 24th 2020 from https://www.sciencedirect.com/science/article/pii/0740624X88900068?via%3Dihub

Salminen, M. 2014. *Mitä "Kyberiä" on turvallisuudessa*? Retrieved September 19th , 2019 from https://politiikasta.fi/mita-kyberia-on-turvallisuudessa/

Sattler, J. 2016. *As cyber threats die, old attacks re-emerge*. Referred January 20th 2020 from https://blog.f-secure.com/as-cyber-threats-die-old-attacks-re-emerge/

Saunders, A , Lewis P & Thornhill, A. 2009. *Research methods for business students.* 5th edition. Pearson Education Limited. Available at:

https://eclass.teicrete.gr/modules/document/file.php/DLH105/Research%20Methods%20for%20Business%20Students%2C%205th%20Edition.pdf

Shorten, A & Smith J. N.d. *Mixed Methods research: expanding the evidence base.* Referred January 23rd 2020. Retrived from https://ebn.bmj.com/content/20/3/74#ref-1

Singh, H. N.d. *A Glance at the United States Cyber Security laws*. Retrieved November 11th 2019. From https://www.appknox.com/blog/united-states-cyber-security-laws

Soft Skills: Definitions and Examples.2020. Article on Indeed career guide's website. Referred April 26th 2020. Retrieved from https://www.indeed.com/career-advice/resumes-cover-letters/soft-skills

Steefkerk, R. 2019. Qualitative vs. quantitative research. Article on scribbr.com's website. Referred January 23th 2020 from https://www.scribbr.com/methodology/qualitative-quantitative-research/

Strategies for Building and Growing Strong cybersecurity Teams: (ISC)² Cybersecurity Workforce Study 2019. 2019. Publication on International Information System Security Certification Consortium's website. Retrieved January 23rd 2020 from https://www.isc2.org/-/media/ISC2/Research/2019-Cybersecurity-Workforce-Study/ISC2-Cybersecurity-Workforce-Study-2019.ashx?la=en&hash=D087F6468B4991E0BEFFC017BC1ADF59CD5A2EF7

Tatham, M. 2018. Identity Theft Statistics. Referred September 26th 2019 from https://www.experian.com/blogs/ask-experian/identity-theft-statistics/

The challenges of cyber security education and training in 2015. 2015. News on Trend Micro's website on March 9th 2015. Referred September 27th 2019 from https://blog.trendmicro.com/the-challenges-of-cyber-security-education-and-training-in-2015/

The National Cybersecurity Workforce Framework. 2017. Publication on National Initiative for Cybersecurity Education website. Referred January 15th 2020 from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf

Top cybersecurity threats in 2020. Publication on University of San Diego's website. Referred January 20th 2020 from

https://onlinedegrees.sandiego.edu/top-cyber-security-threats/

Training. N.d. The Nato Cooperative Cyber Defence Centre of Excellence. Publication on ccdcoe's website. Referred January 20th 2020 from https://ccdcoe.org/training/

Vol. 84, No.152 13884.*Blocking Property of the Government of Venezuela*. 2019. Publication on Federal Register of United States of America Website. Referred October 13th 2019 from https://www.treasury.gov/resource-center/sanctions/Programs/Documents/13884.pdf

Weingarten,J. 2020. All you need to know about the European Credit System ECTS. Accessed April 12th 2020. Retrieved from https://www.mastersportal.com/articles/388/all-you-need-to-know-about-the-european-credit-system-ects.html

World map of encryption laws and policies.N.d. Search engine in Global Partners Digital's website. Referred January 20th 2020 from https://www.gp-digital.org/world-map-of-encryption/

Appendices

Appendix 1. Survey Questions and answer field structures

1. **Which Industry do you work in ?**
-Free text field

2. **Which sector do you work in?**
-Free text field

3. **What is your job title ?**
-Free text field
4. **What is your education ? (ie. MSc in Cyber Security)**
-Free text field
5. **Any non-degree Cyber Security related education ?**
-Multiple-choice checkbox with following choices:
*Certificates
*Cyber Security Related courses
*Hobbies, Events

6. **Is your job management, technical, or a mix (if so, specify weight in "Other", e.g. 40% mgmt, 60% technical) ?**
-Radio button with following choices:
*Management
*Technical
-Free text field on option Other:
*Other

7. **How long have you worked in Cyber Security ?**
-Radio button with following choices:
*0-2 Years
*2-5 Years
*5-10 Years
*10+ Years

8. **For how long have you worked in ICT in general ?**
*0-2 Years
*2-5 Years
*5-10 Years
*10+ Years

9. **List three to five areas of expertise in Cyber Security that you feel most important to perform properly in Cyber Security work.**
-Free text field

10. **If you would now have the opportunity to increase your expertise in three areas in Cyber Security, what would those areas be ?**
-Free text field

11. **As an employee, looking back at the beginning of your career, what Cyber Security skills do you think should have received more attention or more education?**
-Free text field

12. **If you are in a recruiter position, what is the most common area of expertise in Cyber Security among the candidates that is weak or missing ?**
-Free text field

13. **Any other suggestion, how Cyber Security education could be improved ? Opinions regarding all aspects are welcome.**
-Free text field

Appendix 2. University course categorization in NCWF framework

Securely Provision
Risk Management, Risk Analysis, Disaster recovery, Data loss prevention,
Programming, Securing software, Coding, Scripting, Software development, Algorithms
System Architecture, System development, Parallel computing
Identity Management

Operate and Maintain
Data Administration, Databases
Networking, TCP/IP, Protcols, Network Security, Firewalls, IDS, MDM, Routing, Switching
Operating Systems, Server, Applications, Linux, Windows, Unix
Administration, Command line, Practical tools,Cloud Security
Knowledge management
Customer Service and Technical Support
System Analysis

Investigate
Forensics, Investigation
Malware analysis
Reverse Engineering
Malicious Software

Collect and Operate
Collection Operations, Cyber Intelligence, Espionage, Counterfeiting
Cyber Operational Planning, Counter hacking, Conflict, Counter intelligence
Cyber Operations, Electronic Warfare, Cyber operation tools, Surveillance, Reconnaissance

Protect and Defend
Vulnerability assement, Vulnerability analysis, Vulnerability management, Auditing
Incident Handing & Response
Penetration testing, Red teaming, Blue teaming, Purple teaming, Ethical hacking
Endpoint detection & response, Countermeasures, Layered defence

Analyze
Threat Analysis, Threat management, Threat intelligence, Threat modeling
Exploitation Analysis, Data mining
All-Source Analysis, Monitoring, Log, Data Intelligence, Big Data,
Targets, Analytics, Information retrieval, deep learning
Language Analysis, Transaction mining, Fraud detection

Oversee and Govern
Legal Advice and Advocacy, Law, Security Governance, Ethics, Assurance foundations
Training, Education and Awareness, Fundamentals of Cyber Security
Cybersecurity Management, IT Organization management
Strategic Planning and Policy, Security policy, Security planning, Frameworks, TTP, Compliance, Social engineering
Executive Cyber Leadership
Program/Project management and acquisition, Operations management

Appendix 3. NCWF Category numbers explained.

NCWF Categories:	
1	Analyze
2	Collect and Operate
3	Investigate
4	Operate and Maintain
5	Oversee and Govern
6	Protect and Defend
7	Securely Provision

Appendix 4. Survey respondent combined data for most important areas of expertise in Cyber Security.

NCWF Category	Area of Expertise	Number of responses
Undefined	**Soft Skills**	**20**
	Logic, adaptability, team work, Being inquisitive, Ready to learn Ready to accept failure, Systems thinking, critical thinking, sensitivity, Problem solving Quick learner, Holistic view, Communication, Presentation	
4	**Networking**	**14**
	TCP/IP, Networks, Core Internet technologies Understanding TCP-IP, Protocols, Network Security	
7	**Risk Management**	**13**
	Risk Analysis, Risk (all areas), Risk management processes Cybersecurity is all about Risk. Technical knowledge is needed but you need to understand things like BCP, DR, IR, ROI, and how to effectively communicate these to the upper levels and C-Suite. Data loss prevention	
4	**Operating Systems, Server roles & Applications**	**11**
	Application/os stacks, Understanding operating systems and their security controls, Configuration parameters Understanding how webservers and web applications work, Linux&Unix Windows, Understanding how webservers and web applications work	
7	**Programming**	**8**
	Securing Software, Coding, Scripting	
6	**Incident Handling and Response**	**8**
	Incident Handling, Incident Response Procedures	
5	**Education / Training**	**8**
	Employee training, Training in cybersecurity, Education of users End user education, Awareness training, Social engineering	
6	**Penetration testing**	**6**
	Red team, Pentesting	
1,6	**Security / Log analysis**	**6**
	Be able to process large amounts of data and intuitively gather facts, SIEM Logs, Sec monitoring, Data ingestion & Correlation etc	
3	**Forensics**	**4**
	Digital forensics, Artifact knowledge and recovery	
1,2	**Threat Intelligence**	**4**
	Threat identification, Intelligence analysis	
6	**Vulnerability assesment**	**4**
	Vulnerability analysis, Vulnerability management	
5	**Security awareness**	**4**
	Security defaults, Owasp, Security Culture	
7	**Systems Architecture**	**4**
	Systems	
4	**Technical knowledge**	**4**
	Administration skills, System Administration, IT administration experience Strong technical capabilities, Understanding of common IT technologies	
5	**Laws and regulations**	**3**
	Policy & regulations, Data protection regulations	
4	**Crypto**	**3**
	Encryption, Crypto & Understanding of how crypto primitives work together	
5	**Policy & Procedures**	**3**
	Security Policy	
5	**Frameworks**	**3**
	Understanding of NIST controls, Frameworks (Iso27kx)	
5	**Stakeholder processes**	**2**
	Organizational dynamics	
5	**Allaround knowledge of field**	
	General IT Knowledge	

NCWF Category	Area of Expertise	Number of responses
5	**Compliance**	**2**
4	**Configuration documentation & review**	2
	Technical writing	
6	**Countermeasures**	**2**
	Layered Defence	
6,2	**Blue team / defense**	**2**
	Defense OPS	
4	**Infrastructure security**	**2**
	Application / infra hardening	
5	**Security management**	**2**
	Asset Management	
4	**Next Generation Firewalls**	**2**
	Firewall management	
5	**Business management support for cyber security**	**2**
	Defined mission and stakeholders, open communication and buy-in from the business and defined strategy measurement and KPIs	
1,6	**Endpoint Detection & Response**	**1**
4	**MDM solutions**	**1**
7	**Identity Management**	**1**
5	**TTP (Tactics, Techniques and Procedures)**	**1**
2	**Threat Hunting**	**1**
5	**Common mistakes**	**1**
6,2	**Intrusion detection**	**1**
4	**Cloud Security**	**1**
5	**Methods**	**1**
4	**Directory hygiene**	**1**
4	**Orchestration / Automation**	**1**
5	**Social engineering**	**1**
4	**Industrial control Systems (ICS)**	**1**
3	**Reverse engineering**	**1**

Appendix 5. Analyzed and combined data of areas of expertise where questionnaire respondents would educate themselves.

NCWF Category	Area of Expertise	Number of responses
6	**Penetration testing**	**13**
	Offensive hacking, Penetration testing and auditing, Web penetration testing Offensive attacks, Red Team Strategies, Ethical hacking	
4	**Networking**	**8**
	Networking Security	
4	**Technical capabilities**	**7**
	Administration, Server management, Windows OS / Practical tools / Command Line Practical tools, Command Line	
1,6	**Threat and vulnerability management & Analysis**	**6**
	Threat modelling, Insider threat, Threat hunting Threat intelligence analysis, Threat intelligence	
7	**Programming**	**5**
	Low level programming, Programming & Development	
6	**Incident Handling & Response**	**5**
	Incident response processes, Cybersecurity incident management	
3	**Digital Forensics**	**5**
	Cyber forensics	
4	**Cloud Security**	**5**
	Cloud	
4	**Cryptography**	**4**
	Practical encryption usage, PKI	
3	**Malware analysis/Reverse engineering**	**4**
7	**Software security**	**4**
	Application security, Source code security	
1	**Data Analysis**	**4**
	Data classification, Data science, Machine learning, Big data	
7	**Infrastructure security**	**3**
	Architecture, Security architecture	
6	**Blue team**	**3**
	More on defensive cyber security	
4	**Industrial control systems (ICS)**	**3**
	ICS/OT	
1	**SIEM**	**3**
	Monitoring, Logging	
7	**Risk Management**	**3**
	Risk Knowledge, Data loss prevention	
5	**Social engineering**	**2**
6	**Auditing**	**2**
	Secure configuration review, Hosted application audit & Vendor audit	
4	**Automation**	**2**
5	**Education**	**2**
	Become a better test taker	
4	**Next Generation Firewalls**	**1**
4	**Telecommunications**	**1**
4	**Computer engineering**	**1**
4	**Authentication implementation**	**1**
7	**Kernel development**	**1**
7	**Devops**	**1**
5	**Policy writing**	**1**
6	**Attack life cycle**	**1**
5	**For me, all higher level areas. I eventually want to be considered for a CIO position**	**1**
Undefined	**Systems thinking**	**1**
5	**Strategy**	**1**
7	**Business**	**1**
7	**Data science**	**1**
6	**Vulnerabilities**	**1**
5	**Safe behavior**	**1**
1	**Analysis**	**1**
2	**Network security operations**	**1**
6	**Security Controls (CIS)**	**1**

Appendix 6. Analyzed and combined data of areas of Expertise that recruits are most often missing.

NCWF Category	Area of Expertise	Number of responses
Undefined	**Soft Skills**	**8**
	People skills, Interpersonal skills, Systems thinking Common sense, Writing & reading comprehension, Ethics	
4	**Technical capabilities**	**7**
	Technical Depth, Technology, Underwhelming technical skills & knowledge, Systems / Software capabilities, System Administration, Linux	
4	**Networking**	**5**
	Technical understanding of an enterprise network environment and the associated complexities / Interdependencies A strong grasp of network communications	
7	**Programming**	**4**
1	**Threat modeling**	**3**
	Threat understanding, Risk analysis	
6	**Red/Blue teaming**	**1**
7	**The big picture**	**1**
5	**Comptia certifications have no value**	**1**
4	**Real world experience**	**1**
7	**Software architecture**	**1**
7	**An understanding of how cyber security supports the business**	**1**
7	**Security design principles**	**1**
5	**Situational awareness**	**1**

Appendix 7. Analyzed and combined data of areas of areas of Expertise which should had more attention or education in start of the career.

NCWF Category	Area of Expertise	Number of responses
7	**Programming**	**8**
	Programming / Scripting, Basic coding languages, Scripting / Coding	
	Powershell / Python, Programming secure systems	
5	**Business management**	**5**
	Management skills & training, Security culture / Education provided by the company	
	Routines or procedures for certain types of events	
Undefined	**Soft Skills**	**5**
	Self marketing, More confidence when argumenting of security related area with management	
	Handling clients, Communication, Ethics	
4	**Networking**	**4**
	Network Security, Web protocols	
4	**Technical capabilities**	**4**
	Basic system administration & computer skills, Foundational computer science & OS internals	
	Computer science, Security appliance administration	
7, 6	**Basics (Cyber security was not option back in the days)**	**3**
	IT things like continuity planning, Technical monitoring	
	Access management and Vulnerability management	
	Theory and Big Picture ("How to secure a company")	
6	**Penetration testing**	**3**
	Blackhat skills, Thinking like attacker	
7	**Architecture**	**2**
	Security architecture	
4	**Cloud applications**	**2**
	Cloud	
Undefined	**General Mathematics**	**2**
	Math	
5	**Compliance**	**1**
6	**Incident Response**	**1**
	Incident Response Planning	1
1	**Actual analysis**	**1**
7	**Systems development life cycle**	**1**
7	**application security**	**1**
2	**Military**	**1**
7	**Api leverages**	**1**
Undefined	**All skills**	**1**
5	**Real life scenarios**	**1**
7	**Industry trends**	**1**
7	**new technologies**	**1**
7	**Security by design**	**1**
6	**General hardening of applications and infrastructure**	**1**
4	**Orchestration**	**1**
5	**How to raise awareness of issues and remediate in an organisation**	**1**
7	**Risk management**	**1**
	Finding the business impact of security issues	

Appendix 8. Analyzed and combined data of other suggestions, how to improve Cyber Security Education.

NCWF Category	Area of Expertise	Number of responses
4,7	**Core Technical Skills**	5
	More of a focus on core technical skills / Basics. Knowing your systems very very well. If you are a windows shop know windows very very well. A lot of cyber is secure configuration.	
	Learn to code; its an important grounding. Some of these bootcamp snowflakes dont have the points of reference to understand older exploits like buffer overflows let alone aslr	
	Cyber is an IT discipline, but in my experience as a hiring manager, students aren't being given an IT education. They can't tailor their security recommendations based on potential impact to the organization, because they don't understand the underlying technology stack - networking, standard enterprise protocols, etc.	
	Cybersecurity education needs to be layered on top of a software or networking degree	
5,7	**Lifelong learning, Current Technology & Trends**	4
	Students are going to have to have the basic IT and security skills down, but they're also going to need to know how to stay on top of changes in the industry. The landscape shifts so fast that any degree will become quickly obsolete unless they continue their education after graduation.	
	Understand that you can't know everything and that you must constantly improve your skills.	
	Keeping on the edge of the new technology.	
	Using threat intelligence to improve courses to meet better current and future threats	
Undefined	**Soft Skills**	4
	Not neglecting Liberal Arts classes, some more writing classes, Excel skills	
	Develop a training program that focuses on developing problem solving and analytical thinking techniques	
	Ability to break down and relate to non technical people/explaining technical things in a non technical way is huge. Most people don't understand or want to because they don't think it will happen to them until it does.	
	Personally, I would like all programs to have one course dedicated to learning how to get a cybersecurity or IT position out of college. This could include resumes, certification studies, further education, and interviews. Students must be able to figure out what part of the field they want to go into and how their education might fit into that niche as well. A class helping them with the soft skills of the workforce might be able to do exactly that.	
	Develop a training program that focuses on developing problem solving and analytical thinking techniques.	
7	**Business management & Relation to business**	4
	More of a training budget at business / Teach everyone the basic risks	
	Security for the sake of security is pointless. Investment in capabilities without alignment to business goals is pointless. Buyers want good enough, not perfection. Practitioners who want to work in industry need to get educated in business operations on top of developing their CS acumen	
	More socio-technical and user nerd, focusing why security controls help people	
4,6	**Deep knowledge of technology**	3
	More advanced education, more hands-on exercises. Hard to obtain though, as the most skilled people work in private sector instead of education	
	Raise the technical or policy skill bar for graduation. I often interview people with degrees and certs who can't explain the most basic concepts.	
	Linux Cloud	
Undefined	**Specialization**	3
	Security is not just hacking and coding. And also what it definitely is not, is what you see in CSI Cyber. It's also a lot of "boring" stuff as well. It's important to have different kind of cyber experts out there, also for Security management, compliance, architecture and training.	
	Less focus on networking and more on the data	
	All training platforms out there should provide community versions towards Universities. Also, all Universities should have special curriculums.	
5,6	**Real Life Scenarios, Exercises and expectations**	2
	I think, more real exercises on cyber securiry and co-operation with cyber security companies like F-Secure, Nixu, KPMG, Elisa, Telia, DNS etc which companies need to put more efforth on security related areas.	
	Students have high expectations from the complexity of work in infosec. Unless its a position that is deeply specialized, it's going to be mostly about infosec basics and ITIL(or other) framework best practises. Don't get discouraged thought, there is the occational high complexity case where you get to put all you know on the table, and learn more. Learn to absorb the relevant information from lightning fast research.	
5	**Cyber Security Management**	1
	Real world isn't just deploying firewalls and rules, I don't think any of my schooling had incident response or the "managerial" side of things.	
5,7	**Focus equally on public & private sector**	1
	Focus on both public and private sector, including military ops	
6	**Learning both attacker & defender's perspectives**	1
	Learn both perspectives, attackers with incentives and defenders with company regulations	
Undefined	**Clean "non-related" classes from the curriculums**	1
	Too many useless classes that only are in place to fill the requirements. In my bachelors program, I had many classes where I was consistently rolling my eyes and saying "wtf does this have to do with Cybersecurity??"	
5	**Educating young Kids in technology and learn them to be critical about it.**	1

Appendix 9. Response data reflection to curriculum data, most important areas of expertise in Cyber Security

Networking (searchword *network*,*routing*,*switching*,*tcp*)				
	Bachelor EU	Bachelor Usa	Master Eu	Master Usa
Analyze				1
Collect and Operate				**2**
Investigate		7	1	4
Operate and Maintain	49	28	38	40
Oversee and Govern				
Protect and Defend	3		1	2
Securely Provision	1			
Nature S	**42**	**22**	**21**	**18**
Nature S/E	3	8	11	27
Nature CB	1	3		
Nature E	7		8	
Nature not described		2		4
Programmes	13	15	16	17

Risk Management (searchword *risk*)				
	Bachelor EU	Bachelor Usa	Master Eu	Master Usa
Analyze			1	
Collect and Operate				
Investigate				
Operate and Maintain				
Oversee and Govern		1	5	
Protect and Defend				
Securely Provision	3	5	12	10
Nature S	**2**	**3**	**14**	**5**
Nature S/E		3	1	1
Nature CB				
Nature E	1		3	4
Nature not described				
Programmes	3	5	9	9

Operating systems, server roles & applications (searchwords *Linux*, *Windows*, *Unix*, *Operating Systems*, *Database* , server*, administra*, *command line*, *practical tool				
	Bachelor EU	Bachelor Usa	Master Eu	Master Usa
Analyze				
Collect and Operate	**1**			
Investigate		2		1
Operate and Maintain	30	30	16	23
Oversee and Govern				
Protect and Defend				
Securely Provision	2	1		3
Nature S		**22**	**11**	**7**
Nature S/E		4	1	
Nature CB		4		
Nature E			4	20
Nature not described		3		
Programmes	12	13	6	11

Programming (searchword *programming*, *Java*, *Ruby*, *Python*, *C#*,*C++*,*JS,*software dev*)				
	Bachelor EU	Bachelor Usa	Master Eu	Master Usa
Analyze				
Collect and Operate				
Investigate				1
Operate and Maintain				
Oversee and Govern				
Protect and Defend				
Securely Provision	55	28	27	4
Nature S	**26**	**18**	**7**	
Nature S/E	9	5	10	
Nature CB	3	4		
Nature E	18		9	5
Nature not described		1	1	
Programmes	14	13	9	5

Incident Response (searchword *incident*)				
	Bachelor EU	Bachelor Usa	Master Eu	Master Usa
Analyze				
Collect and Operate				
Investigate	1	1	1	1
Operate and Maintain				
Oversee and Govern				
Protect and Defend	2	1	4	5
Securely Provision				
Nature S	**1**	**2**	**4**	**3**
Nature S/E				
Nature CB				
Nature E	2		1	3
Nature not described				
Programmes	3	2	4	4

Education/Training (searchword *education*	Bachelor EU	Bachelor Usa	Master Eu	Master Usa
	Bachelor EU	**Bachelor Usa**	**Master Eu**	**Master Usa**
Analyze				
Collect and Operate				
Investigate				
Operate and Maintain				
Oversee and Govern	1			1
Protect and Defend				
Securely Provision				
Nature S				**1**
Nature S/E				
Nature CB				
Nature E	1			
Nature not described				
Programmes	1			1

Penetration testing (searchword *penetration*, *red team*, *ethical*)				
	Bachelor EU	**Bachelor Usa**	**Master Eu**	**Master Usa**
Analyze				
Collect and Operate				
Investigate				
Operate and Maintain				
Oversee and Govern	1			
Protect and Defend	14	7	7	8
Securely Provision				
Nature S	**12**	**5**	**5**	**2**
Nature S/E	1	1	1	
Nature CB	1			
Nature E	1	1	1	6
Nature not described				
Programmes	11	7	6	4

log / security analysis (searchword log*, *security ana*, *siem*,*monitoring*,*ingestion*,*correlation*,*data analysis*,*traffic analysis*,*big data*)				
	Bachelor EU	**Bachelor Usa**	**Master Eu**	**Master Usa**
Analyze	3	1	6	7
Collect and Operate				
Investigate		2		
Operate and Maintain			2	
Oversee and Govern				
Protect and Defend			2	1
Securely Provision		1		
Nature S	**1**	**4**	**4**	
Nature S/E			3	
Nature CB				
Nature E	2		3	8
Nature not described				
Programmes	3	3	8	5

forensics (searchword *forensic*)				
	Bachelor EU	**Bachelor Usa**	**Master Eu**	**Master Usa**
Analyze				
Collect and Operate				
Investigate	12	29	11	18
Operate and Maintain				
Oversee and Govern				
Protect and Defend	1			
Securely Provision				
Nature S	**12**	**19**	**7**	**3**
Nature S/E	1	4	2	
Nature CB		1		
Nature E		2	2	15
Nature not described		3		
Programmes	9	14	10	11

Appendix 10. Response data to curriculum data reflection, areas of expertise to be increased

Threat analysis & management (searchword *threat*,*Insider*)				
	Bachelor EU	Bachelor Usa	Master Eu	Master Usa
Analyze			1	1
Collect and Operate				
Investigate				
Operate and Maintain			1	
Oversee and Govern				
Protect and Defend		1		2
Securely Provision			1	1
Nature S		**1**	**2**	
Nature S/E				2
Nature CB				
Nature E			1	2
Nature not described				
Programmes	0	1	3	3
cloud security (searchword *cloud*)				
	Bachelor EU	Bachelor Usa	Master Eu	Master Usa
Analyze				
Collect and Operate				
Investigate				
Operate and Maintain	4	1	5	6
Oversee and Govern				
Protect and Defend				
Securely Provision				
Nature S	**3**	**1**	**3**	**1**
Nature S/E			1	
Nature CB				
Nature E	1		1	3
Nature not described				2
Programmes	4	1	4	5

Appendix 11. Response data to curriculum data reflection, skills requiring more attention at the start of career

Business management (searchword *business*)										
	Bachelor EU		Bachelor Usa		Master Eu		Master Usa			
Analyze										
Collect and Operate					**1**					
Investigate										
Operate and Maintain										
Oversee and Govern					3		3			
Protect and Defend										
Securely Provision			2				3			
Unrelated			**7**		**6**		**5**			
Nature S			3		3		1			
Nature S/E			2		4		1		8	
Nature CB			1							
Nature E			2		1		9			
Nature not described			1		2					
Programmes	0		7		6		8			

Appendix 12. Response data, bacground information of respondents, questions 1-8

Industry	Count of Responses
ICT & Telecommunications	28
Military	2
Financial	3
Health Care / Pharmaceutical	4
Retail	2
Education	3
Government	1
Car industry	1
Job Title	
Manager positions	14
Architecht / Technical Lead	5
Specialist / Analyst / Engineer / Consultant	20
Instructor	2
Trainee	2
Classified military ranks	1
Working sector	**Count of Responses**
Private	28
Other	1
Public	15
Education	**Count of Responses**
Bachelor in other ICT	16
Master in Cyber/Information Security	8
Bachelor in Cyber/Information Security	6
Master in other ICT	4
No degree	4
Master in Business Administration	2
Bachelor in Business Administration	2
Bachelor in Economics	1
Bachleor in Psychology	1
Associate in Cyber/Information Security	1
Bachelor in Political Science	1
Bachelor in Mathematics	1
Bachelor in Industrial management	1
Bachelor in Social Science	1
Juris Doctor in Law	1
Bachelor in Communication and English	1
Graduate Certificate in Cyber Security	1
Bachelor in Electrical Engineering	1
Doctoral candidate in Cyber Security	1
Non-Degree Cyber Security related education	**Count of Responses**
Certificates	29
Cyber Security Related courses	29
Hobbies, Events	28
Work Distribution	**Count of Responses**
Technical	17
Management 25%, Technical 75%	2
Management 30%, Technical 70%	2
Management 40%, Technical 60%	2
Management 50%, Technical 50%	2
Management 70%, Technical 30%	3
Management 90%, Technical 10%	1
Management	13
Management & Technical, no distribution specified	1

Career duration in Cyber Security	Count of Responses
0-2 Years	**13**
2-5 Years	**12**
5-10 Years	**9**
10+ Years	**10**
Career duration in ICT	**Count of Responses**
0-2 Years	**9**
2-5 Years	**2**
5-10 Years	**13**
10+ Years	**20**

Appendix 13. Raw data

Collected curriculum and questionnaire raw data available here:

https://gitlab.labranet.jamk.fi/cs4e/examination-of-contemporary-cyber-security-education/-/tree/master/Raw%20data

Collected curriculum and questionnaire manipulated and categorized data available here:

https://gitlab.labranet.jamk.fi/cs4e/examination-of-contemporary-cyber-security-education/-/tree/master/Manipulated%20data